Automating the Thin Blue Line: Controversy, Knowledge, and the Governance of Police Technology in Canada

by

Daniel Konikoff

A thesis submitted in conformity with the requirements for the degree of Doctor of Philosophy
Centre for Criminology and Sociolegal Studies
University of Toronto

© Copyright by Daniel Konikoff (2024)

Automating the Thin Blue Line: Controversy, Knowledge, and the Governance of Police Technology in Canada

Daniel Konikoff
Doctor of Philosophy
Centre for Criminology & Sociolegal Studies
University of Toronto
2024

Abstract

In 2020, journalists uncovered that Canadian police services had surreptitiously acquired, used, and lied about Clearview AI, an invasive facial recognition technology. The revelations sparked controversy, revealing gaps in how police technology is regulated in Canada. This project uses the Clearview AI controversy to explore the social, political, legal, and cultural challenges that police technology poses for Canadian governance regimes. Drawing upon scholarship from policing studies, governance studies, and science and technology studies, this project argues that attempts at governing police technology in Canada fail due to police secrecy, ambiguities at the intersection of the public and private sector, and a patchwork of bodies and institutions with incomplete regulatory authority over both policing and technology.

Automating the Thin Blue Line explores these issues through ethnographic observations, content analysis of nearly a hundred government documents, and over 50 interviews with stakeholders from policing, government, civil society, and private industry. This project shows how the Clearview AI controversy revealed previously unexplored gaps in how police buy, use, and control cutting-edge technology. It also demonstrates how controversies shape technological governance, arguing that police departments across Canada responded to this controversy by mounting seemingly collaborative governance initiatives with advocacy groups, governmental bodies, and the Canadian public. My project finds that these initiatives failed to materialize

because of asymmetrical power relations that favour police and private industry, resulting in governance mechanisms that are collaborative in name alone. I also engage reflexively with my own challenges accessing research participants from police departments, demonstrating how governance initiatives are often framed as attempting to dismantle—but ultimately cannot overcome—the culture of secrecy and inaccessibility that pervades policing. These issues put police's regulatory identity in crisis: police wind up caught between the rule-bound bureaucracy of the public sector and the move-fast-and-break-things ethos of private technology companies. Overall, this project uses empirical exploration to showcase the growing range of relevant actors involved in police technology's governance. It uses this vantage point to examine not only top-down dynamics of cooperation, knowledge governance, and controversy closure between these relevant actors, but also the friction, disagreement, and distrust that characterizes their relationships.

Acknowledgements

To everyone who's ever asked me at a party, "What is it that you do, exactly?"

To everyone who ever followed up that question with, "What do you do after you get your degree?"

To everyone who further clarified their question by asking, "So you're *not* going to be a lawyer?"

***

To Rebekah, who has stuck around in Toronto far longer than she's wanted to while I've completed this thing. To my sisters, Marlee and Lauren, who served as brainstorming partners throughout my project, and who bought me bubble tea on bad days. To my dog, Meadow, who encouraged me to take frequent breaks with her requests to play fetch, and to my cat, Moon, who'd rub her face on my laptop until I'd scratch her. To my dad, who encouraged me not to go to law school, and to my mom, who can now say that her son is a doctor. To my best and oldest buds, Matthew Jordan and Julian Muia, who I could always rely on for proofreading or jamming or both. And to all the wonderful friends who have supported me along the way with drams of whiskey, rounds of D&D, meals, chats, movie watch parties, and general encouragements of "you can do it": Elizabeth Al-Jbouri, Alex Barnes, Eileen Church Carson, Liam Crummey, Renato D'Ambrosio, Kira Feldman, Loretta Kerr D'Ambrosio, and Josh Newman.

To faculty past and present who have guided me along the way: Rosemary Gartner, who hosted me for lovely dinners and told me that a good dissertation is a done dissertation; William Watson, who has been both my biggest academic champion and my favourite person with whom to gab pop culture; to Akwasi Owusu-Bempah, Patrick Watson, and Keith Guzik, who have been beyond helpful intellectually, professionally, and emotionally; to Mary X. Mitchell, who saved this project on countless occasions while still finding time to flood my inbox with hot takes about the state of modern music; and to Beatrice Jauregui, who's been saddled with me since my MA but who's been nothing but generous with her time, instrumental in fostering my intellectual interests, and whose catchphrase of "This is a good start" has always helped set a fire beneath me when inspiration was low. To Joshua Shaw, a once-and-future collaborator who has warmly shared his wisdom for every issue, no matter how small, I've ever had about academia. And to my colleagues at CrimSL: my mentors Giancarlo Fiorella, Jihyun Kwon, and Grace Tran; my brilliant cohort mates Fernando Avila, Tyler King, Kadija Lodge-Tulloch, and Jona Zyfi; and my dear pals Laura Acosta Zárate, Olivia Berkovits, Jamie Duncan, Huibin Lin, Alex Luscombe, Adina Radosh, Roxy Shlapak, Diego Tuesta, and Jeffrey Wong, who have been the best partners in criminology anyone could ever ask for.

***

To my silly brain, which thought it'd be a good idea to write the acknowledgements before I even wrote the dissertation. Maybe this is exactly the motivation it needs to wrap this thing up: if I've written *something*, even the acknowledgements, then how hard can it be to write the rest?

Table of Contents

LIST OF ACRONYMS VI

INTRODUCTION: AUTOMATING THE THIN BLUE LINE 1

Methodology 5
Literature Review 8
a. Governance, Networked and Collaborative 8
b. Policing: Technology, Reform, Transparency 10
c. STS: Controversy, Systems, and the Politics of Knowledge 13
Plan of the Dissertation 18

CHAPTER 1: CLEARVIEW AI AND THE TECHNOLOGICAL CRISIS IN CANADIAN POLICING 20

"The Secretive Company That Might End Privacy As We Know It" 21
Situating Journalists in Expanding Governance Networks of Police Technology 27
Controversy and Tension within Governance Responses to Clearview AI 36
a. The TPSB's Use of AI Policy, and the TPS' AI Procedure 36
b. Provincial, territorial, and federal joint guidance and open letter on facial recognition in policing 41
c. The RCMP's National Technology Onboarding Program 47
Conclusion 52

CHAPTER 2: PARSING GAPS AND ASYMMETRIES WITHIN THE POLICE-TECH-GOVERNANCE PATCHWORK 54

The False Promise of Governance 56
a. Regulatory Gaps External to Policing 56
b. Regulatory Gaps within Policing 67
c. Collaborations as Reinforcements of Police Power and Autonomy 72
Conclusion 80

CHAPTER 3: BLUE WALLS, BLACK BOXES, AND THE POLITICS OF KNOWLEDGE IN POLICE TECHNOLOGY 82

Constructing Ignorance, Marketing Transparency 83
The Architecture of Secrecy 89
The Imbalanced Politics of Transparency and Trust 98
The Police Technology Knowledge Playbook 106
Conclusion 108

CHAPTER 4: GOVERNING TECH WHERE PUBLIC AND PRIVATE COLLIDE 110

The Challenge of Public-Private Innovation in Uncertain Regulatory Space 116
a. Innovation and Regulation at Odds 116
b. The Encroaching Private Sector on Public Police Technology 127
Conclusion 136

CONCLUSION: GOVERNING THE (AUTOMATED) THIN BLUE LINE 138

Implications and Directions for Future Research 140
a. Expanded Case Studies and Refinement of Controversy's Source 140
b. Comparative Research on Hard Law 141
c. Theorizing and Testing Best Practices for Improved Stakeholder Engagement 142
d. Public Surveys on Correlations between Trust, Legitimacy, and Knowledge 143
e. The Viability of Alternate Modes of AI Governance 143

POSTSCRIPT: PACKING UP THE BLACK BOX 147

REFERENCES 148

List of Acronyms

Access to Information program (ATIP)
Artificial Intelligence Technology Committee (AITC)
American Civil Liberties Union (ACLU)
Artificial Intelligence (AI)
Algorithmic Impact Assessment (AIA)
Automated fingerprint identification system (AFIS)
Automated license plate reader (ALPR)
Canadian Association of Chiefs of Police (CACP)
Canadian Association of Police Governance (CAPG)
Child Exploitation Services (CES)
Facial recognition technology (FRT)
Information and Privacy Commissioner of Ontario (IPC)
International Association of Chiefs of Police (IACP)
Members of Parliament (MPs),
National Technology Onboarding Program (NTOP)
New York Police Department (NYPD)
Office of the Privacy Commissioner of Canada (OPC)
On-device investigation tool (ODIT)
Ontario Digital Service (ODS)
Ontario Human Rights Commission (OHRC)
Ontario Police Services Act (OPSA)
Ontario Provincial Police (OPP)
Public Oversight of Surveillance Technology Act (POST)
Privacy Impact Assessment (PIA)
Royal Canadian Mounted Police (RCMP)
Technology Services Division (TSD)
Toronto Police Service (TPS)
Toronto Police Service Board (TPSB)
Treasury Board Secretariat (TBS)

Introduction: Automating the Thin Blue Line

"Push button to play polka."

This was the sign beside the escalator that led down to the Wisconsin Conference Centre, located in Milwaukee's downtown core. In May of 2022, Milwaukee was playing host to the International Association of Chiefs of Police's (IACP) annual Technology Conference, and I was there for what promotional conference email blasts had hyped up as "the premier professional event dedicated to discussing technology in law enforcement." I got off the escalator and followed the decidedly un-policelike music (Whitney Houston's "I Wanna Dance With Somebody," Marvin Gaye and Tammi Terrell's "Ain't No Mountain High Enough") to the conference centre's ballroom, where representatives from law enforcement agencies the world over—mostly from the US and Canada, but also from Nigeria, Colombia, Israel, the United Kingdom, and the Netherlands—had gathered for the conference's opening ceremony.

The topic of this year's gathering was the governance of police technology and the challenges that emerging technologies pose for public trust in policing. Three administrators from American policing were onstage to deliver the keynote. Chief Dwight Henninger of the Vail Police Department, Chief Jeffrey Norman of the Milwaukee Police Department, and acting director of the Department of Justice's COPS Office Rob Chapman iterated, reiterated, and re-reiterated that when it came to technology, police had a responsibility to innovate with community trust in mind. Chief Henninger, appraising technology and trust in synergy, proclaimed that technology "enables, constrains, and defines policing in our communities," and that "there is nothing more important to policing than trust-building." He finished with what would become a mantra repeated over the next three days: "Police have a responsibility to use technology thoughtfully."

Over the past few years, police departments across North America and beyond have demonstrated a "ready, fire, aim" mentality with digital technology. Government, civil society, the public, and police agencies themselves have been left to reckon with how to best control police technologies before they go awry, and have been left wondering how best to pick up the pieces of technologies that already have. Whether it be the myriad articles revealing international police departments' surreptitious (and occasionally inaccurate) use of facial recognition software (Harwell, *Washington Post,* April 13, 2021), increased awareness around the risks that data-driven police technology poses to constitutional rights (Diaz, *Brookings,* September 13, 2021), or police

departments from the US to Germany to Israel testing and deploying spyware on political dissidents (Cox, 2022; Deutsche Welle, 2022; Haaretz, 2023), law enforcement agencies have shown the ease with which dangerous technologies can be deployed without public awareness and without guardrails governing their use, all in the name of public safety.

This dissertation explores how technological projects have emerged as common points of contention in Canadian policing. Over the last decade, municipal, provincial, and federal agencies have courted scandal any time 'policing' and 'technology have found themselves in the same sentence. Some have found that simply *proposing* the acquisition of bleeding-edge digital tools is cause for conflict. In the summer of 2018, amid rising gun crime, the Toronto Police Service (TPS) found themselves in hot water when they proposed the purchase of ShotSpotter, an automated gunshot detection system. The proposal incited protest from civil liberties organizations and members of Toronto City Council, who objected to ShotSpotter's ability to capture street-level conversations. And between May and July of 2023, Hamilton Police Service, located just 70 kilometres west of Toronto, was in the news for their plans to expand their drone program (Mitchell, *Global*, May 29, 2023). This plan incurred the ire of community groups and privacy advocates, who expressed concerns about drones' capacity for expanding surveillance power. Though neither ShotSpotter nor the drone program materialized, the suggestion of an increasingly technologized police force stirred conflict among stakeholders.

Another source of controversy has been police's quiet acquisition—often accompanied by loud denial—of cutting-edge digital technology. One notable scandal arose around International Mobile Subscriber Identity (IMSI) catchers. Also known as Stingrays, IMSI catchers are cellphone tower emulators for eavesdropping and intercepting mobile phone traffic. The TPS, Ontario Provincial Police (OPP), and the Royal Canadian Mounted Police (RCMP) denied using the privacy-invasive technology, but pressure and investigation from reporters, civil society, and government ultimately forced the agencies to backtrack. In 2020, the University of Toronto's Citizen Lab, an academic research lab that studies the intersection of technology and human rights, released a report mapping Canadian police's use of predictive policing tools, highlighting the risks that algorithmic policing and automated surveillance tools can pose for privacy and equality (Robertson, Khoo, & Song, 2020). In July 2022, the RCMP got in trouble again with activists and experts for their otherwise undisclosed use of "on-device investigative tools" (ODITs, also known as spyware) to surveil the Canadian public (Cecco, *The Guardian*, July 8, 2022). Throughout

Ontario, various detachments of the OPP have started expanding closed-circuit television (CCTV) camera coverage in small towns despite these towns' low crime rates and ill-defined political motivations for these cameras' acquisition (Bedford, *The Recorder & Times*, September 20, 2023). And with the OPP's expansion of the CAMSafe program, an online police registry for home security cameras, some have suggested that Ontario's provincial police force is normalizing ambient surveillance networks across suburbs and cities (Cooper, *CTV News*, November 6, 2023).

This project focuses on the leadup to and fallout over one of the more consequential police technology scandals in recent memory: that of Clearview AI. In early 2020, the TPS, OPP, and RCMP made headlines for using Clearview AI's facial recognition technology (FRT). Built on a database of over 3 billion photos of people's faces taken from the internet without people's consent or awareness, Clearview AI's FRT had made its way into police departments without the awareness of ranked superiors, and its existence and use were denied to the public (Aguilar, *City News*, February 13, 2020). The controversy that ensued brought renewed attention to Canadian police's habit of keeping acquisition and use of invasive technologies a secret. More importantly, the controversy exposed regulatory gaps in how police technology and FRT are governed both within and outside police departments.

Governance of police technology is an important and timely topic of study at a moment marked by rapid development of sophisticated computing and artificial intelligence (AI) tools. The Clearview AI controversy provides a perfect prism for analyzing how police governance of technological change in Canada functions and whom it serves. For one, the Clearview AI controversy reveals the limits of existing governance structures around both policing and technology. It also points to the regulatory tensions that arise at the peculiar nexus between the governance of policing, on the one hand, and the governance of technology, on the other. Further, the controversy surfaces which actors, groups, and institutions have a stake in questions of police technology's governance, while highlighting the conflicts, tensions, debates, and disagreements that arise between stakeholders in question.

To that end, the Clearview AI controversy points to a subject that remains underexplored in policing scholarship: police technology and technology governance regimes as sources of civil disagreement and distrust. Scholars have highlighted a crisis of trust in North American policing, largely to do with long-simmering concerns surrounding racially biased enforcement practices and excessive, occasionally lethal use of physical force (Koper & Lum, 2019; Weisburd & Braga,

2019; Wortley & Owusu-Bempah, 2022). Research has highlighted police technology as a threat to civil rights and liberties, particularly for vulnerable populations, but has paid less attention to fleshing out the controversies that bubble up around these technologies, and how issues of trust arise from these tools' usage (Bacchini & Lorusso, 2019; Eubanks, 2018; Moy, 2021).

Examining waning stakeholder trust in police is especially important in the context of police's often clandestine adoption and use of technologies, which raise new questions about transparency and accountability in policing. Police in Canada have demonstrated a tendency to keep external stakeholders in the dark about the technologies in their arsenal, what these tools do and do not do, what their intended or unintended consequences may be, and how much they are costing taxpayers (Bloch-Wehba, 2021; Koningisor, 2023; Manes, 2019). Coupled with the newfound ubiquity of AI in all aspects of social life, police's growing attraction to AI-enabled technologies, and public and governmental distrust in AI writ large, it is imperative to study the police's use of AI is as a site of conflict and as a site of reform (Isaac, 2017; Joh, 2019).

My project takes the Clearview controversy as a jumping-off point for exploring how municipal, provincial, and federal stakeholders in Canada debate, adopt, control, and contest emerging, sophisticated police computing and information technologies. To crack open this question and more, I examined police services and institutions across three levels of Canadian government. The police departments I assessed had all recently been in the crosshairs of controversy for their surreptitious use of Clearview AI's powerful, privacy invasive FRT, and the institutions I analyzed all had a stake in the governance of policing, technology, or both. The agencies I chose to investigate were the TPS and its related oversight body, the Toronto Police Services Board (TPSB); the Ontario Provincial Police (OPP); and the Royal Canadian Mounted Police (RCMP). Not only had these forces all been revealed to have been using Clearview AI in secret, but they had all been part of a post-Clearview wave of governance initiatives that emerged in response to the scandal. This furnishes a rich entry point for my exploration of how FRT and AI are governed in the context of policing on municipal, provincial, and federal scales. These governance initiatives include:

1. **Municipal:** the TPSB's Use of Artificial Intelligence Policy (hereby referred to as the TPSB AI Policy) and the TPS' Artificial Intelligence Technology Procedure (hereby referred to as the TPS AI Procedure).

2. **Provincial:** joint guidance and a recommended legal framework on police's use of FRT in Canada, done in collaboration between Canada's provincial, territorial, and federal privacy commissioners.
3. **Federal:** the RCMP's establishment of the National Technology Onboarding Program (NTOP), designed to standardize and centralize technology acquisition, use, and governance across the force.

By exploring the Clearview AI controversy through institutions at three levels of government, I analyze the ways different actors and groups have approached governance reform in the wake of public controversy. This enables me to unpack how the stakeholder groups who orbit police technologies play roles in developing or contesting technological governance. As a result, I argue that attempts to govern police technology through regulatory fixes often fail. These reforms struggle to address deeper issues within Canadian law and policing, such as legacy legal regimes that are poorly fitted to new technologies, as well as self-regulatory practices that allow police to reject consultation and feedback from external stakeholders. Further, I argue that attempts to govern police technology are often stymied by police's claims to expertise surrounding police technology, and the architecture of secrecy that police erect around this knowledge to maintain their knowledge's primacy. Finally, the relationship between police departments and private technology vendors shows how the regulations of public organizations often clash with the cutting-edge expectations of private enterprise, leaving police caught between the rule-bound bureaucracy of the public sector and the move-fast-and-break-things ethos of private enterprise. Overall, the world of police technology is a world of conflict, and the reforms that emerge to mend these conflicts often amount to little but empty promises.

Methodology

This study employs mixed qualitative methods, including semi-structured interviews, participant observation, and document analysis.

In keeping up with police technology controversies in Canada through public fora, I began sketching out a collection of distinct but intertwined stakeholders I saw as playing a part—however big, however small—within how police technology is acquired, contested, and governed. These stakeholders are united by their intimate familiarity with some aspect or aspects of the broader

world of police technology in Canada, even if their roles and functions within that world are different.

I developed a breakdown of relevant stakeholder groups and interviewed participants from each. Overall, I conducted 53 interviews with 54 interlocutors from these stakeholder groups: police consultants (n=3), privacy offices (n=9), police departments (n=11), policing- and technology-related advocacy groups (n=7), crime, technology, and security journalism (n=5), police professional associations (n=2), Canadian governmental bodies (n=7), police technology companies (n=9), and police boards (n=1). I spoke to most individual stakeholders only once; two of my interlocutors I interviewed twice, and there were three interviews in which I interviewed duos. Except where participants asked to be identified, I have kept their identities and participation confidential. Where possible, I worked with participants to co-develop nomenclature that sufficiently captures their stakeholder group and profession without compromising their personal identities (i.e., senior police official from Ontario, co-founder of a police software start-up, security reporter for a Canadian newspaper, etc.).[1] When relating data gathered from participants in this project, I use the gender-neutral pronoun "they" to further protect participant anonymity.

In preliminary discussions, I asked these stakeholders to tell me about their professional experience working in the world of police technology, getting a glimpse into some of the questions and concerns that crop up among real people working in this space. These conversations helped me tease out the parameters of my project and formulate my research questions, while leading me to other stakeholders I had not yet considered. Once I had transcribed all my interviews, I uploaded the transcripts into NVivo and began a grounded approach to coding and analysis. This grounded approach allowed themes and categories to emerge from the interview data, which were then identified as 'codes' that succinctly summarized the emerging ideas and concepts (Allan, 2003). Once I finished sorting interview data into themes, I analyzed each theme to identify patterns in participant responses.

I utilized document analysis to inform and contextualize interview data. Publicly accessible documents like technology policies, transcripts from police board meetings and government

[1] A key stakeholder that is missing here is the public—the people who will be most affected by the police use of facial recognition. As I will discuss later, I was able to capture a sliver of data from the public through some publicly available documents. Nevertheless, an interesting consequence of not being able to conduct a wider survey on this was that I was able to see how different stakeholder groups see their work in relation to the public, and how these different stakeholders make sense of the public's understandings of facial recognition.

debates, public consultation submissions, patent applications, and newspaper reportage all provided valuable insights and helped me track the development of ongoing police technology controversies. However, much of the information I sought was not available for public disclosure, given the secretive nature of policing as an institution and the sensitive nature of the processes undergirding the acquisition, use, and governance of police technology. I submitted Freedom of Information (FOI) requests to four institutions—the TPS and TPSB, the OPP by way of the Ministry of the Solicitor General, the RCMP, as well as the Office of the Privacy Commissioner of Canada (OPC)—to gather data that shed light on these institutions' inner bureaucratic functioning. My FOIs to the TPS and OPP yielded little, but I did receive a 450-page disclosure from the RCMP regarding NTOP, as well as a 500-page disclosure from the OPC regarding their development of joint FRT guidance. These documents provide insight into the behind-the-scenes conversations and machinations that go into building a police technology governance mechanism from scratch.

Further, I conducted participant observation at in-person and online sites that are relevant to either the sale or governance of police technology. Ultimately, I attended virtual police board meetings (n=5), police association webinars (n=3), and a City of Toronto procurement information session (n=1). I also attended the IACP's 2022 Technology Conference. I sat in on panels, visited vendor booths in the exhibit hall, and networked with attendees, observing an understudied yet significant venue where police technologies are discussed and, most relevantly, bought.[2]

Through interviews, document analysis, and ethnography, I have developed a preliminary picture of the world of police technology in Canada, and of the tensions that exist between police technology stakeholders. Interviewees shed light on the competing interests undergirding police technology's regulation, while documents and observation spotlight the many ways in which thoughtful technological governance is so hard to come by. My data tells a story of police caught between its public mandate and private industry, policing and governmental bodies lost in the

[2] In parsing out this world of police technology, it occurred to me that the ideal research experience would be to conduct ethnographic observation in police departments' units that pertained to technology. In October 2021, I submitted Applications to Conduct Research with both the TPS and the York Region Police (YRP), but since I had been cautioned that these application processes could take a long time, I sought out other observation sites while waiting for the cogs of bureaucracy to churn in my favour. Ultimately, nearly two years after I submitted my application to the TPS, the TPS denied my application to conduct research with them. YRP approved my application, but shortly after approval, my primary YRP contact stopped responding to my emails, and my research window expired before I could re-establish contact.

chasms between patchwork regulations, and a confluence of stakeholders divided by competing conceptions not only of governance but of technology itself.

Literature Review

a. Governance, Networked and Collaborative

This dissertation engages with governance literatures to understand how police technology is and is not regulated. Governance and public administration scholars have noted that governance is a broad concept referring to the structures, systems, and practices that control or direct organizations and entities (Cleveland, 1972; Levi-Faur, 2012; Poluha & Rosendahl, 2012). Governance is often concerned with how decisions are made, who has a voice in making these decisions, and who is ultimately held accountable in decision-making processes (Bevir, 2012; Levi-Faur, 2012). Understood as "processes of rule wherever they occur," governance is not only comprised of institutions and actors, but also tangible artifacts like policies, procedures, frameworks, and laws that steer the decisions of institutions (Ansell & Torfing, 2022; Bevir, 2012, p. 1; Pierre & Peters, 2020).

Governance, in these literatures, appears to be many things at once. It is a structure, comprised of bodies and institutions which themselves employ people; it is a process; it is something that is 'done' or 'performed' by *x* over (or for, or against) *y*; and it is materials, a collection of rules and regulations and acts and mandates which hold governing power in and of themselves and which guide governance processes. Governance is also an outcome, the result of materials and processes and structures working in tandem to impose order and control on phenomena. Governance thus comes in all shapes and sizes. State government or not, any organization or institution that is run well (or at least tries to run well) needs governance to function (Ansell & Torfing, 2022; Bevir, 2012; Levi-Faur, 2012; Pierre & Peters, 2020). Governance scholarship thus provides a helpful frame for discussions of police technology: it helps capture the multiplicity of actors and institutions involved in governing police technology, the processes these actors and institutions embark upon to fulfill regulatory functions, and the varying artifacts that these actors and institutions follow or create in bringing control to police technology.

This study also draws on and contributes to scholarships on collaborative network governance as a means of accounting for the work of numerous communities of actors working across different scales of governance (Agranoff & McGuire, 2001; Gash, 2022; Keast, 2022;

Rhodes, 1996; Wang & Ran, 2021). Compared to more traditional scholarship on governance, this body of work focuses on the "the presence of diverse components" within governance networks, especially on the relevance of non-state actors (Klijn & Koppenjan, 2014, p. 61). This focus typifies the field's emphasis on "complexity": governance is a dynamic affair, characterized by shifting stakeholder relationships on the route to securing successful regulatory outcomes (ibid.).

Though scholars from public administration, governance studies, political science, and public policy studies have come to understand network governance and collaborative governance as separate concepts, these scholars recognize that both concepts are premised upon the importance of coordination and interdependence in achieving collective objects (Agranoff & McGuire, 2001; Bevir, 2012; Gash, 2022; Keast, 2022; Rhodes, 1996; Wang & Ran, 2021). Definitions of both concepts emphasize what Wang & Ran (2022) call "collective decision-making process for public service delivery" (p. 1187). Both concepts foreground the decision-making processes of governance as premised on reciprocity, sharing power, building trust, and achieving consensus via negotiation (Ansell & Gash, 2008; Emerson, Nabatchi & Balogh, 2012; Fadda & Rotondo, 2020; Fischer, 2012; Isett et al., 2011; Provan & Kenis, 2008; Wang & Ran, 2021). Deliberation, crucial in both network and collaborative models of governance-making, is premised on the diversity among collective stakeholders, and is thus inclusive and egalitarian (ibid.). And though network governance scholarship is more likely than collaborative governance research to point out the tensions and power imbalances between actors in governance networks, these tensions and power imbalances are framed in the context of *managing* tensions and *achieving* successful governance, rather than leading to their outright failure (Cleveland, 1972; Hermansson, 2016; Purdy, 2012; Ran & Qi, 2019). Looking at the Clearview AI controversy helps develop this aspect of network governance scholarship, showing how multi-actor, multi-institution systems can fail at regulating police technology, allowing technology like Clearview AI's FRT to slip through gaps in Canada's regulatory patchwork.[3]

[3] Similar yet is emerging scholarship on AI governance, which describes governance as a multi-modal affair made up of actors from across government, industry, and civil society, as well as a number of initiatives and artifacts (Andrey et al., 2023; Kuziemski & Misuraca, 2020; Wareham et al., 2014). Many chapters within the recently published *Oxford Handbook of AI Governance* (2023) discuss the necessity of a theoretical framework that captures stakeholder complexity within AI regulatory schemes (Dafoe, 2023); provides templates for "multi-stakeholder convening" in the development of AI policy (Greene, 2023); unpacks power inequalities between stakeholders within the AI governance ecosystem (Lazar, 2023); and the tensions that arise between public and private sector stakeholders when public organizations use and govern AI (Bullock et al., 2023).

A small section of scholarship looks to network and collaborative governance in policing. Most scholarship about the governance of police primarily has to do with police's interaction with government and external bodies in the context of formal accountability processes, and focuses on the procedures and methods that ensure police are doing their job properly (Clarke, 2009; Goldsmith & Lewis, 2000; Ingrams, 2017; Livingston, 2004; Morton, 2019; Nalla & Mamayek, 2013; Prenzler, 2015; Prenzler & den Heyer, 2015; Rossler & Terrill, 2012; Savage, 2015; Sen, 2010; Walker, 2005; Walsh & Conway, 2011). However, a burgeoning literature has come to apply network and collaborative governance theories to police. Some scholars use these theories to unpack how police collaborate with state and non-state actors to bolster their own accountability, while others use these concepts to tease out the partnerships police forge with public and private actors to provide social control to hard-to-reach populations and spaces (Aditya & Kusumastuti, 2023; Brewer, 2014; Lee, 2021; Li, 2017; Paasche, 2013). *Automating the Thin Blue Line* is a contribution to this growing area of study. It is one of the first studies to explore network and collaborative governance in issues surrounding police technology, and it articulates the structures of interdependence that serve as sights for police technology to fail and for new governance mechanisms to be created.

b. Policing: Technology, Reform, Transparency

Automating the Thin Blue Line contributes to the vibrant and diverse body of criminological scholarship examining the intersection of policing and technology, and expands it to focus more specifically on the ways in which the governance of police technology is created and contested. After all, police have long been fascinated with technological innovation. From patrol wagons to squad cars, call boxes to two-way radios, batons to firearms to TASERs—extensive scholarship has chronicled the ways different technologies have, for better or worse, revolutionized police practice and organization (Chan, 2001; Deflem & Chicoine, 2014; Harris, 2007; Johnson, 1981 Maguire & King 2004; Manning, 1992; Manwaring-White, 1983; Walton, 1982). In addition, much of these scholars' efforts have been devoted to exploring whether technological innovation in policing actually works, conducting research to determine if certain tools have made officers more responsive, their enforcement more effective, and their investigations more efficient (Koper & Lum, 2019; Manning, 1992; Nunn, 2001). But only some subsets of scholarship—most notably research exploring whether body-worn cameras (BWCs) enhance police accountability—have

focused explicitly on the intersection of police technology and governance (Ariel et al., 2017; Hyatt, Mitchell & Ariel, 2017; Koen & Mathna, 2019; Mateescu & Rosenblat, 2016; Wright & Houston, 2021). This project contributes to the wider scholarship on police technology by focusing specifically on police use of FRT and AI-driven tools but expands this scholarship's scope to wrestle more explicitly with the regulatory debates that swirl around police technology.

One of the ways *Automating the Thin Blue Line* does this is by situating institutional responses to the Clearview AI controversy within scholarship on police reform. Many scholars have studied the variegated strategies stakeholders adopt to try and change policing (Huey, Ferguson & Schulenberg, 2023; Rosenbaum & Lurigio, 1994; Skogan, 2008; Walker, 2016). Police reform can take any number of shapes, from police professionalization initiatives to the establishment of community policing practices, but a common theme across the police reform literature is reforms' origins. These works highlight how police reform often emerges from moments of crisis, unfolding in response to specific dilemmas and problems in law enforcement (Bayley, 2008; Skogan, 2008; Walker, 1977; Weisburd & Braga, 2019; Worden & McLean, 2017). *Automating the Thin Blue Line* contributes to this literature by showing how the Clearview AI controversy surfaced problems with police technology that new governance models were established to reform.

Further, by focusing on the impact of police keeping Clearview AI a secret, my project engages with policing literatures on the complex interplay between technology, transparency, and secrecy. Secrecy is one of the earliest subjects of study in policing scholarship. Starting with William A. Westley's (1956) landmark research on the 'blue wall of silence,' police scholars have highlighted secrecy as a feature, not a bug, of police's occupational culture (Chin & Wells, 1997; Conway & Westmarland, 2021; Koepke, 1999; Liu, 2020; Powers Jr., 2000). It is no secret that many aspects of policing still unfold, well, in secret. Many legal scholars writing about policing have shown how secrecy is not only built into police culture, but supported by legal infrastructure like Fourth Amendment doctrine, non-disclosure legislation, and executive protections (Bloch-Wehba, 2021; Friedman & Janszky, 2020; Koningisor, 2020; Koningisor, 2023).[4] *Automating the*

[4] Scholars have floated different terms to speak to chronic police secrecy. Bloch-Wehba (2021) refers to it as police's "opacity problem," Friedman & Janszky (2020) call it "policing's information problem," and Chanin & Espinosa (2015) call it police's "long-standing preference for reticence" (p. 3). Koningisor (2023) discusses this phenomenon as "police secrecy exceptionalism," referring to the "unique secrecy protections" afforded to police (p. 615).

Thin Blue Line echoes this scholarship about police secrecy by emphasizing both the cultural and structural conditions that allow secrecy around police technology to flourish. This project builds on the secrecy literature and connects it to scholarship within the interdisciplinary field of science and technology studies (STS) by explaining how technological secrecy becomes both a source of controversy as well as a tool that constructs and defines police authority.

Just as my project engages with research on police secrecy, it also engages with research on police transparency. Transparency is a valued feature of democratic governance premised on opening aspects of policing up to public observation. This scholarship has explored and sometimes critiqued efforts to render transparent things like police policies, procedures, crime data, departmental information, and on-the-ground police decision-making (Ingrams, 2017; Mason, Hillenbrand & Money, 2014; Schafer, 2013; Tregle, Nix & Pickett, 2022). Some scholars have recognized the instrumental value police may ascribe to transparency, arguing that police departments may communicate proactively with the public in order to bolster police legitimacy (Brainerd & Edlins, 2015; Chermak & Weiss, 2005; Crump, 2011; Heverin & Zach, 2010; Mawby, 2010; Unsworth, 2014). Other scholars have framed transparency by highlighting a more manipulative side of public disclosure, recognizing that police organizations may use transparency and information sharing as a public relations tool meant to manage narratives about the police and protect the department's reputation (Chanin & Espinosa, 2016; Mawby & Worthington, 2002; O'Connor, 2017). What is more, some scholars have used transparency as a frame for discussing police technology, exploring how tools like predictive policing software, BWCs, digital surveillance infrastructure, smartphones, and social media can render police performance more transparent (Bakke, 2018; Brucato, 2015; Chanin & Courts, 2017; Manes, 2019; Stone, 2018).

This project does not engage with the notion of technology as a tool for greater police transparency. Rather, it analyzes how existent governance models created conditions for police in Canada to use technology *without* transparency, and how governance models that emerged in the wake of Clearview AI were positioned (but struggled) to address this secrecy. It also draws attention to the instrumental value of transparency policy, showing how in some cases, police position new governance around police technology as a way of fulfilling reputational goals in an attempt to win back public trust.

This project thus intervenes in research on the complex interplay between trust, transparency, and technology in policing. Scholars have suggested that greater transparency

around police operations in general can help bolster citizens' trust in policing (Jackson, 2015; Kochel & Skogan, 2021; Mason, Hillenbrand & Money, 2014; Zheng, 2023). Relatedly, research on FRT (Bradford et al., 2020), BWCs (Crow, Snyder, Critchlow & Smykla, 2017), drones (Heen, Lieberman & Miethe, 2018; Sakiyama, Miethe, Lieberman, Heen & Tuttle, 2017), CCTV cameras (Gurinskaya, 2020), and algorithmic decision-making (Hobson, Yesberg, Bradford & Jackson, 2021; Selwyn & Gallo Cordoba, 2021) has shown that increased trust in policing institution can positively influence public acceptance of police's use of technology, and decrease concerns the public might have about different types of technology. *Automating the Thin Blue Line* further enriches this perspective, exploring how both police and civil society navigate widespread distrust in both policing *and* technology, and how trust factors into the success or failure of technology governance regimes.

Overall, this project expands policing literatures to account for the complex interplay between cutting-edge technology and transparency, trust, and reform. It contributes to the police technology scholarship by exploring police's secretive use of FRT, its implications for trust and transparency, and FRT as a source of controversy. This project also deepens the literature on police reform by exploring how new governance models emerged in the wake of Clearview AI as concrete reforms meant to quell a crisis of waning public trust and a crisis of secrecy and transparency. Further, it synthesizes this perspective with network and collaborative forms of governance to explain how stakeholders contest technological controversy and collaborate on attempting to mount reforms to technological governance.

c. STS: Controversy, Systems, and the Politics of Knowledge

Historians and sociologists of science and technology employ a rich toolkit that can supplement exploration of technology governance in policing. This project draws on three such tools: controversy, the politics of knowledge, and sociotechnical systems.

Historians of science and technology have found controversy to be a helpful entry point into exploring the complex relationships between technology and society (Bijker & Pinch, 1987; Epstein, 1996; Jasanoff, 2012; Nelkin, 1971; Nelkin, 1974). These scholars have argued that the sociological history of technology is shaped by controversies, or disagreements arising between different social groups and actors who hold different ideas about technological or scientific phenomena (Collins, 1975; Pinch, 1977, 1986; Pickering, 1984). The disagreements that make up

controversy are analytically essential: examining conflict and controversy has a unique power to expose the full range of actors, communities, and artifacts at play in an issue (Callon & Rip, 1992; Venturini, 2010). What is more, science and technology scholars have pointed to the concept of *closure* to explore how conflicts between stakeholders in sociotechnical systems can be brought to an end or manipulated to remain open (Klein & Kleinman, 2002; Pinch & Bijker, 1987).

This project uses controversy over police technology as an analytical window into Canada's technology governance regimes. Focusing on Canadian police's controversial use of Clearview AI's FRT allows for more careful analysis of who has a stake in debates around police technology, how existing governance regimes failed to regulate technology, and how a diverse set of stakeholders develop and contest new modes of technological governance in policing. Further, bringing the analytical frame of controversy into conversation with network and collaborative governance explored in the previous section allows for the inclusion of a fuller range of social groups into this analysis, including people affected by the technologies, and puts a greater premium on the tensions, conflicts, and disagreements between actors and institutions in their pursuit of governance. Exploring controversy helps enrich literatures on police reform by showing how reform efforts do not necessarily or universally bring closure to a conflict. As I show in what follows, governance interventions such as the Toronto policing institutions' AI Policy and Procedure, the privacy commissioners' guidance and recommended legal framework on FRT, and the RCMP's creation of NTOP were created to bring closure to public controversy over Clearview AI. However, these reform responses just as often telegraphed to civil society stakeholders some of the essential and profound ongoing problems with police technology governance.

Further, this project enhances its exploration of police secrecy and transparency by engaging with the politics of knowledge, most specifically the concept of *agnotology*. Agnotology explores how the construction of ignorance, uncertainty, unknowledge, and doubt is part and parcel of knowledge-making (Proctor & Schiebinger 2008). Whereas studies of knowledge production largely focus on 'how we know what we know,' agnotology asks 'why don't we know what we don't know,' and supposes that institutions and groups also produce and maintain ignorance as a part of broader politics of knowledge (Crawford, 2022; Kourany & Carrier, 2020; Proctor & Schiebinger, 2008). Most notably, scholars writing on the politics of knowledge argue that ignorance and unknowing are "made, maintained, and manipulated by means of certain arts and sciences" in a process referred to as *agnogenesis* (Proctor & Schiebinger, 2008, p. 15). This is not

so much an innocuous gap in available knowledge within a certain field, but rather an active production of ignorance by a wilful party. Further, studies of agnotology do not just pay attention to who produces ignorance and how it is produced, but also for whom and against whom is this constructed ignorance deployed, asking, 'Who is ignorant, why, and for whose benefit?'

The agnotology literature thus offers powerful tools for exploring the sociology and politics of knowledge in policing. In policing literatures, knowledge has traditionally been framed through police's status as "knowledge workers" collect and process vast amounts of information for investigating criminal activity and fulfilling security functions (Brodeur & Dupont, 2006; Ericson & Haggerty, 1997). However, this project focuses less on the information police use in their day-to-day operations and more on the higher-level knowledge comprising police expertise on technology. And though scholars like Tombs and White (2003), as well as Barton and Davis (2018) have applied agnotology to criminal justice issues, there is no scholarship applying agnotology to policing, nor to the study of police technology. This project finds great value in agnotology, which helps refine understandings of the Clearview AI controversy and the secrecy at the heart of police technology as the product of deliberate ignorance-making.

Further, looking at the politics of knowledge helps us refine our engagement with network and collaborative governance literatures, which conceive of knowledge and information as resources to be shared between governance actors (Agranoff & McGuire, 2001; Bevir, 2012; Gash, 2022; Keast, 2022; Rhodes, 1996; Wang & Ran, 2021). However, these governance literatures do not focus as much on networks premised on *secrecy*, where knowledge is shared among some stakeholders but withheld deliberately from others. In conversation with network and collaborative governance, agnotology helps explain how different stakeholders are kept in the dark about police technology, and how withholding knowledge about police technology ultimately impacts the way technology is governed.

Moreover, understanding the politics of knowledge surrounding police technology and its governance points to the jurisdictional claims police institutions make about authority over the technologies in their digital armoury. STS scholars, most notably Sheila Jasanoff, have explored the contested processes through which emerging technologies and expert knowledges are governed. As Jasanoff (1990) notes in her book *The Fifth Branch*, regulatory agencies tasked with presiding over scientific and technological change have turned to expert communities to legitimate these agencies' engagements with emerging knowledges (Jasanoff, 1990). Jasanoff (1990) points

specifically to scientific advisory committees—including science advisors and technical experts—as playing an essential role in shaping government agencies' regulatory processes. But digital police technologies like FRT fit poorly into the types of regulatory frameworks Jasanoff outlines; after all, police's relationship to technology is not as an expert group layered between branches of government, but as technology's *user*. Here, Oudshoorn & Pinch's (2003) observation that 'users matter' is instructive. Police institutions are an important class of users of emerging technologies such as FRT, and it is through their use of these technologies that are available to them and them alone that police come to claim expert knowledge over these tools. The politics of knowledge and governance surrounding police technology, therefore, are intimately entwined with police institutions' professional jurisdiction (Abbott, 1988). This study therefore explores the interplay between the ways in which technologies simultaneously become part of the police occupational toolkit *and* become objects through which police articulate claims of exclusive occupational jurisdiction. This shows how police assert the primacy of their own knowledge and expertise around FRT in governance processes.

Jurisdictional struggles over FRT and police technology open questions of public communication and public trust. As I will show, police institutions often claim that police technologies are critical parts of their exclusive occupational toolkit, which must sometimes be kept secret to ensure that bad actors cannot circumvent their use. These claims undergird arguments that members of the public should trust in police expertise and accept police's judgments about their own secrecy as coming from a place of authority. But as STS scholars have shown across numerous studies, public trust in experts and technical expertise is fragile, as debates have arisen around whether experts should be given privileged positions within democratic processes (Brunk, 2006; Grundmann, 2016; Hawley, 2012; Wynne, 2006). Public trust in policing, meanwhile, has been on the wane in light of poor police performance, questions about law enforcement organizations' integrity, high-profile instances of police misconduct, and extensive histories of racial bias.

This study explores how multiple aspects of police technology governance and public understandings around it—namely the role of journalists in translating knowledge about police technology to the public, as well as stakeholder engagement in the creation of police technology governance—has been informed by what STS scholars call a 'deficit model' (Brunk, 2006; Lewenstein, 2003; Wynne, 2006). In general terms, deficit models assume that members of the

public are uninformed about science and technology, and that they require 'experts' to educate them. However, the hierarchical, 'public deficit' framing of public understanding, Wynne (2006) explains, often backfires by failing to address sources of public mistrust, and in so doing can even catalyze further distrust. These dynamics are well explored in controversies over scientific knowledges about issues such as pesticides (Blok, Jensen & Kaltoft, 2006; Wynne, 2001) and nuclear contamination (Durant, 2007; Otway, 1992). My study suggests they are increasingly at play in controversy over emerging police technologies. It explores how police institutions' claims of jurisdiction and models of public engagement both respond and contribute to problems of public trust, keeping controversy over FRT from closing and driving a seemingly relentless churn of reform proposals.

In applying select STS concepts to the study of the governance of police technology, this project ultimately contributes to the diverse body of scholarship examining the intersection of science, technology, and justice. Scholars like Cole (2002), Egbert & Leese (2021), Guzik (2016),[5] and Lokaneeta (2020) have looked at how technological innovations have transformed expressions of governance, social control, and state power in the contexts of national security, policing, and legal systems. Most important, these scholars' works recognize the complex entanglements of sociotechnical systems (Borrás & Edlar, 2014): that technology is best understood through the actors and institutions who use it, the social context in which it is deployed, and the political aims that it is trying to achieve. Compared to studies of governance of policing institutions, and especially models of network and collaborative governance, this project uses empirical exploration to showcase the wide and growing range of relevant actors involved in police technology's governance. It uses this vantage point to examine not only top-down dynamics of cooperation, knowledge governance, and controversy closure between these relevant actors, but also the friction, disagreement, and distrust that characterizes their relationships. *Automating the Thin Blue Line*, like the works mentioned above, engages with the materiality of Clearview AI's FRT as a technology, but situates it within the broader sociotechnical network of which it is a part.

[5] Similar to Guzik's (2016) *Making Things Stick*, this project explores the ways in which the governance regimes that emerged in light of the Clearview AI controversy have—like the three surveillance programs Guzik describes as Mexico's attempts at surveilling mobility, communication, and identification—failed to live up to expectations.

Plan of the Dissertation

This project is divided into four chapters. In Chapter 1, I explain the Clearview AI controversy in greater detail and situate it within a brief history of the use of FRT in law enforcement. Drawing upon controversy, I argue for an expansion of the categories of actors and institutions commonly included in conceptions of network and collaborative governance. I show how journalists played a vital, but heretofore underexplored, role in surfacing the main points of contention in the Clearview AI controversy—namely, the fact that the tool was built on a database of illicitly gathered photographs, as well as the tool's use by police without public disclosure. Then, I explain the emergence of regulatory reforms across municipal, provincial, and federal levels. Drawing again on controversy and complex governance models, I show how these new modes of governance sought to bring closure to the Clearview AI controversy, but in so doing further highlighted conflicts and tensions between key stakeholders.

In Ch. 2, I explore the fractured and patchworked approach to police and technology governance that preceded and conditioned the Clearview AI controversy. Specifically, I show that the laws, policies, and institutions—which preceded and continue to exist in the wake of the Clearview AI controversy—failed to forestall the problems showcased by the controversy in the first place. I also demonstrate how these laws, policies, and institutions continue to be ill-equipped in Clearview's wake, as they struggle to meaningfully govern the complex and ambiguous regulatory intersection of policing and technology. Ultimately, I argue that these governance practices inhere within and even create asymmetrical power relations that systemically favour Canadian police actors, allowing them unfair advantage to set their own governance agenda around their use of technology.

In Ch. 3, I explore the relevance of the politics of knowledge through discussions of technological transparency and secrecy. While governance efforts are positioned as rendering police use of advanced technology more transparent, I argue that these efforts cannot overcome the architectures of secrecy that pervade police departments and technology companies. I draw on agnotology to unpack how legal and political structures—such as non-disclosure agreements, procurement by-laws, freedom of information (FOI) legislation—allow police to acquire technology in secret and withhold necessary knowledge about technology from the public. This chapter uses the politics of knowledge to further explore how police departments assert primacy

of their own technological knowledge to ultimately stymie meaningful collaboration with other stakeholders on the development of technological governance.

Finally, in Ch. 4, I unpack the tension that arises between public and private interests and explore some of the key challenges that emerge when governance and innovation intersect in policing. By exploring this tension through the eyes of police technology vendors and police administrators, I argue that the governance of police technology winds up caught between the rule-bound bureaucracy of the public sector and the move-fast-and-break-things ethos of private enterprise. I conclude this section by highlighting how in police's struggle to live up to their ambitions as technological innovators, police departments have started coopting some of the hallmarks of the private sector. As part of this, police have begun framing technology governance reforms as innovations in and of themselves.

By focusing on one of the most notable police scandals of the 21st century, *Automating the Thin Blue Line* demonstrates how police technology has become a cause of controversy and a troublesome thing to control. Governing the messy nexus where policing and technology meet has proven hard work, sparking conflict, entrenching law enforcement secrecy, and reasserting the dominance of private companies and police departments alike.

Chapter 1: Clearview AI and the Technological Crisis in Canadian Policing

The first day of IACP panels kicks off with "Drone Operations in Public Safety: Use Cases, Lessons Learned and Strategies for Implementation." The conference room is filled wall-to-wall with officers so giddy that you would think they were talking about flying RC planes for fun, not work, but one person—a police officer in the crowd who identifies as hailing from Seattle—is decrying how off-putting the technology is to those outside of policing. The officer laments that if he had suggested drones for *his* unit, in *his* city, he would be "slapped around." The panelists nod in support and paint a picture of the technology as mired in controversy. One panelist says, "If you just buy a drone, and get a whole team, and don't tell anyone, you'll pay the piper later." To "do drones right," they continue, you need to build clear policies around "the things that the detractors didn't want to see." "We won't weaponize drones," they say, "we don't use ALPRs on drones, no facial recognition." The mention of facial recognition sets the room to squirming. Sensing this wave of unease, the panelist breaks into an easy smile and jokingly throws the conversation to a member of the crowd who had chimed in earlier. "Seattle—are you using facial rec?" Seattle responds with an incredulous laugh. "I'm not even allowed to say the word."

The word follows me to my next panel, "Turning Face: Ethical Use of Facial Recognition." At the front of the room is a retired cop who is now the co-founder of the National Child Protection Task Force, which provides expertise and resources to police investigating cases with missing and trafficked children. After regaling a rapt audience with a story about how facial recognition technology (FRT) helped him find an abused kid from a cold case "in seconds," the panelist makes an impassioned plea for the value of the technology. Facial recognition is "worth everything," the panelist says, and police "*must* use this stuff—but we have to be better at it." They give the audience a knowing wink, as if they are all in on a joke. "Am I allowed to say Clearview? Is that a bad word? Will I get arrested for it?" A room full of police officers snigger in unison as the panelist makes an aside that cuts through the laughter: "Clearview. The evil word."

This chapter takes this "evil word" as its jumping-off point to examine Clearview AI explore how controversy over its early, clandestine use inflected the broader governance of police technology in Canada. Tracing the Clearview AI controversy and its immediate impacts on Canadian policing, this chapter argues for the utility of the Clearview AI controversy as an analytical point of entry into the governance of police technology: it helped expose regulatory gaps

in existing governance models, it served as a catalyst for regulatory reform, and it surfaced a constellation of unexpected actors (and the tensions between them) in exercises of governing police technology.

My exploration of the Clearview controversy enriches scholarly literatures on network and collaborative governance in two ways. First, my analysis shows how a wide range of stakeholders beyond policing and government institutions play important roles in the governance of police technology. Although actors like journalists are not commonly regarded as relevant stakeholders in scholarly literatures on collaborative and network governance, their intervention in the Clearview controversy had important and direct effects on governance responses. Second, I demonstrate how governance responses to the Clearview controversy at the municipal, provincial, and federal levels complicate theoretical understandings of network and collaborative governance as premised on "trust, power-sharing, diversity, consensus, inclusiveness, deliberativeness [and equality]" by highlighting the importance of stakeholder friction and conflict to police technology governance (Emerson, Nabatchi & Balogh, 2012; Provan & Kenis, 2008; Wang & Ran, 2021).

The chapter begins by situating Clearview AI within a brief recounting of FRT's history, before explaining what made law enforcement's use of Clearview AI so controversial in the first place. Then, it highlights the importance of journalists as important actors in the governance models that emerged in response to Clearview AI (Fadda & Rotondo, 2020; Isett et al., 2011; Provan & Kenis, 2008). The chapter concludes by exploring these governance models, looking at how institutions at three separate levels of government—Toronto police institutions, the Royal Canadian Mounted Police (RCMP), and Canada's provincial, territorial, and federal privacy commissioners—crafted unique responses to the regulatory gaps surfaced by investigative reporting on the Clearview AI controversy. By fleshing out how these institutions sought to regulate FRT and artificial intelligence (AI) more broadly, this section will chronicle moments of collaboration and friction within these governance models, showing the different shapes governance can take in the wake of controversy.

"The Secretive Company That Might End Privacy As We Know It"

FRT is a controversial tool in policing's arsenal, but few companies are as controversial as Clearview AI, the company behind one of the most notorious police technologies to date. Yet Clearview AI's FRT is not entirely an anomaly within the wider history of police technology. It is

the culmination of mathematical research into facial recognition, and its existence is consistent with public safety agencies' centuries-old fascination with biometrics and facial identification. What makes Clearview AI so distinct and its use in Canadian law enforcement particularly controversial comes down to two factors: the privacy-violating nature of the technology itself, which relies on photos taken from the Internet without people's consent, as well as the police's use of this technology with minimal transparency and accountability.

The connection between criminality and images of the human face dates to 1852, when prisons in England capitalized on the advent of photography to take pictures of inmates to improve record-keeping and assist with tracking escapees (Raviv, January 21, 2020). In post-Civil War United States, the Pinkerton National Detective Agency, one of America's first formalized law enforcement organizations, began taking pictures of people they apprehended and used these pictures as the basis for their "Rogues Gallery," the first criminal mugshot database (Pinkerton, "Our Story," n.d.). Though systematized and automated techniques for actually matching people to photos had yet to be fully developed, the core of these early efforts was the compilation of databases, comprised exclusively of pictures of people who had already come into contact with the criminal justice system.

The ability to match two images of the same person's face to one another improved in 1963, when mathematician Woody Bledsoe and his company Panoramic Research Incorporated set out to conduct "a study to determine the feasibility of a simplified facial recognition machine" (Raviv, January 21, 2020). Bledsoe's experiments relied on machine reading and automated pattern recognition: Bledsoe began building a system that could read or 'understand' new inputs, recognize key components within them, and determine whether they aligned with a set of images on which the system had already been trained (ibid.). Once this machine was built, Bledsoe attempted to train a computer to recognize a database of 10 photos, each showing a different person's face, and see if the machine could then recognize new photos of those same people.

After several failed attempts, Bledsoe revised the machine reading system by taking inspiration from the anthropometric work of Alphonse Bertillon. A French criminologist and one of the pioneers of the modern mugshot, Bertillon had developed a comparison system that involved measuring the distances between major facial features like eyes, ears, nose, eyebrows, and lips. It used those distances between major markers to generate unique identifiers, almost like fingerprinting but for the face (Cole, 2002). This technique worked better for Bledsoe and his team,

but the new facial recognition machine still struggled to manage the fundamental variability of the human face. The machine worked well when fed new pictures that were similar enough to those from the training database, but the machine faltered when fed photos of those same people with different facial expressions, facial hair, or signs of aging (Raviv, January 21, 2020).

A new injection of funding from the US government drove further development of Bledsoe's system. In 1967, shortly after Bledsoe's work with Panoramic Research dissolved, Bledsoe began tinkering with facial recognition again on a contract funded by the Central Intelligence Agency (CIA), the United States' civilian foreign intelligence service (Raviv, January 21, 2020). Bledsoe's CIA contract was meant to produce FRT to help police match suspect portraits against mugshot databases. His experiments proved fruitful, with the machines he developed vastly outpacing humans at correctly and efficiently identifying new pictures of suspected criminals against an existing database of criminal mugshots (ibid.).

Bledsoe's work on facial recognition ultimately plateaued by the late 1960s, but his research laid the groundwork for mathematicians and engineers throughout the 1970s, 80s, and 90s to further refine facial recognition technologies. Building off of Bledsoe's experiments and capitalizing on developments in computing power and linear algebra, these researchers expanded the number of facial markers that computers could identify and developed mathematical techniques to make these processes capable of automatic identification—laying the groundwork for the likes of Clearview AI to emerge some years later (Goldstein, Harmon & Lesk, 1971; Sirovich & Kirby, 1987; Turk & Pentland, 1991).[6]

The connection between public safety institutions and FRT grew dramatically during 90s and early 2000s. In the early 1990s, the United States' Defense Advanced Research Projects Agency (DARPA), a department responsible for developing emerging technologies for military use, launched the Face Recognition Technology (FERET) program. The program was meant to compile a large database of facial images that FRT developers could use to train their technologies, all for spurring greater innovation in FRT, expanding FRT's commercial market, and creating FRT products for public safety (NEC, May 12, 2022).

[6] For more on this history, see Goldstein, Harmon & Lesk's (1971) development of a 21-point facial measurement system, Sirovich & Kirby's (1987) advances in using linear algebra in visually representing pictures of faces, and Turk & Pentland's (1991) eigenface technique for algebraically recognizing faces in real time.

With the establishment of the FERET program, the market for FRT continued to expand, as had its increased use in policing and public safety strategy. Although these tools were controversial, the use of FRT and the identity of the companies providing FRT were, to an extent, public information. Moreover, the databases on which these tools ran were limited in scope, comprised exclusively of images of criminal suspects.

FRT became more controversial after the press broke news of its use as a general surveillance tool at the 2001 Super Bowl. Three days after the game, the *Tampa Bay Times* broke the story that police had used cameras from defence contractor Raytheon and FRT vendor Viisage, and that they had linked these cameras to a police control room inside the stadium (Trigaux, January 31, 2001). The cameras captured the faces of each of the 100,000 fans that went through the turnstiles at Raymond James Stadium, and "each facial image was digitized and checked electronically against the computer files of known criminals, terrorists and con artists of the Tampa Police Department, the FBI and other state and local law enforcement agencies" (Trigaux, January 31, 2001). The use of FRT at the 2001 Super Bowl kicked up a flood of controversy, with members of the public and civil society decrying FRT as a new and urgent threat to personal liberty and privacy (Hill, 2023). Controversy deepened in Tampa a few months later when the Tampa City Council acquired facial recognition software from Visionics Inc. and approved a pilot to combine FRT with CCTV cameras in the Tampa neighbourhood of Ybor City (Gates, 2011; Moore, July 12, 2001). Still, however, Visionics was by then a known actor, its use in Tampa was transparent and under the oversight of local government, and its capabilities were restricted to images contained within Florida mugshot databases.

North American public opinion towards FRT softened after the terrorist attacks of September 11, 2001. In the post-9/11 political landscape, US lawmakers and security agencies put a greater premium on increased public safety at the expense of privacy, and technologically advanced surveillance capabilities became more and more appealing to a wider array of actors (Gates, 2006). This acceptance reached its apex in October 2001 when the US Congress signed into law the *USA Patriot Act*, which included "a mandate that the government assess the accuracy of biometric tracking technologies, including facial recognition technology" (Hill, 2023, p. 64). From there, stock prices for surveillance companies surged, as law enforcement and security agencies spent the coming decades testing FRT's viability and implementing FRT into policing and public safety operations (ibid.).

As private companies increasingly dominated the world of police surveillance technology, these companies further pushed their surveillance tools 'underground.' Private companies were able to exert greater pressure on police to keep proprietary surveillance technologies secret (Joh, 2017). Police institutions, meanwhile, came to regard their use of these tools as something to obfuscate lest criminals be given undue advantage (Manes, 2019).

Separately, the widespread public recognition of the longstanding problem of racialized police violence in the 2010s sparked mounting calls for greater transparency in police operations, including in the arena of police technology. Following the 2014 murder of Michael Brown by Officer Darren Wilson in Ferguson, Missouri, then President Barack Obama launched the President's Task Force on 21st-Century Policing, which identified widening rifts between law enforcement and the communities they serve, citing a crisis of waning public trust. The Task Force's final report identified several corrective measures for improving policing post-Ferguson, such as having clear and comprehensive policies and data on their operations, as well as encouraging police to adopt radical disclosure and access provisions to make these policies and data more transparent (Task Force, 2015). Most notably, the report identified "the centrality of technology in policing" and technology's potential to "improve policing practices and build community trust and legitimacy," but noted that police departments hoping to use technology need to "work with the public and other partners in the justice system" to ensure that police technology is used with public awareness and governed by rigorous transparency standards (Task Force, 2015, pp. 31-32).[7]

Calls for greater police transparency in the United States reverberated within Canada. In a 2020 report, the RCMP identified what they observed to be a greater public desire for police transparency. "Political pressures, social change and a more vigilant and involved public," went the report, have impacted the trust that Canadians have for their police forces and all levels of government. Changing perceptions have created the requirement for increased transparency and openness on the part of our public institutions" (RCMP, Environmental Scan, 2020, p. 16). Overall, while policing grew more and more technologized, and while much of this technologization

[7] As part of the President's Task Force on 21st-Century Policing, President Obama proposed an investment of $263 million to improve law enforcement training and equip 50,000 police officers with BWCs. This speaks to the stock that stakeholders put into technological reforms in the wake of crises in policing.

unfolded out of the public eye, the public, civil society, and government actors were putting greater stock in police transparency.

By the time Clearview AI entered the FRT market, it was offering something different from many of its FRT predecessors—something far more privacy-invasive, and something far more secret. Founded in 2017 by Australian entrepreneur Hoan Ton-That and former American politician Richard Schwartz, Clearview AI was, first and foremost, built upon developments in the field of AI, specifically neural networks, in which machines can learn to perform tasks in a manner like that of the human brain (Gurney, 2018). But whereas previous FRT had limited police to databases of government-born images like mugshots or driver's license photos, Clearview had engineered a system that built a database by automatically collecting images (otherwise referred to as "scraping") of people's faces from the Internet (Kurenkov, January 15, 2022). Clearview's scraping algorithm combed social media sites like Facebook, YouTube, Twitter, Instagram, and American mobile payment service Venmo, as well as websites dedicated to employment, news, and education, all to scoop up images for the company's ever-blooming database. Clearview's tool allowed users to then upload pictures of their own for comparison against this vast trove of scraped biometric data. Clearview marketed their FRT system to law enforcement, offering police the capability of identifying suspects, victims, or anyone for whom they had a picture, by matching those photos to people's online profiles. By the time Clearview AI started making its way into law enforcement agencies, it had far exceeded the more contained mugshot databases of FRT's yesteryear: Clearview had amassed a database of more than 3 billion photos of people's faces, all taken from the Internet.[8]

Unlike the Viisages and Visionics that had made headlines in the United States in the early 2000s, Clearview AI managed to evade public scrutiny in its first few years on the market, operating in relative secrecy but making tremendous headway into law enforcement agencies around the world. Clearview's first client was the New York Police Department's Financial Crimes Unit, and from there, the tool spread by word of mouth through the rest of the NYPD's ranks and beyond (Hill, 2023). Soon, Clearview AI had law enforcement in a grip; the US' Federal Bureau of Investigation (FBI) and Homeland Security were using it, as was the international law enforcement coordination group Interpol, the Australian Federal Police, and the Royal Canadian

[8] At the time of this writing, Clearview AI's database contains as many as 20 billion photos of people's faces scraped from the internet.

Mounted Police (RCMP) (ibid.). Investigators at agencies who were using Clearview's state-of-the-art FRT were calling Clearview "the biggest breakthrough in the last decade," especially for solving some of policing's most heinous cases like child abuse and sexual exploitation (Hill & Dance, February 7, 2020). Clearview had proved that its unique affordances—matching a picture of anyone against a massive database of illicitly harvested photos linked to people's online profiles—was appealing to law enforcement, but also something that, given past public and civil society outcry about FRT, was worth keeping hidden from view.

Clearview AI thus proved to be a concerning tool arriving at a time of changing public attitudes toward policing and technology. Clearview AI's FRT owed much to the technologies that came before it, but it differentiated itself by being built off images automatically culled from the open web. This new capability presented police with unprecedented power in facial identification, which had only a few years prior been limited to databases within police or government control. And though police's secretive use of Clearview was not much different from their secretive purchase and use of other surveillance technologies, Clearview's existence in the shadows of police departments came at a time of increased desire for police transparency—and as we will see, was something police felt they had to actively obscure.

Situating Journalists in Expanding Governance Networks of Police Technology

Amidst this rise in police secrecy around technology, as well as wider public sentiment pushing police toward greater transparency, investigative reporters served an essential role in surfacing the Clearview AI controversy and rendering its use transparent. By making otherwise opaque police practices visible, investigative journalists helped expose regulatory gaps in how institutional actors in policing and beyond governed (or failed to govern) FRT and AI. The work of journalists directly catalyzed reforms to governance regimes, showcasing how journalist joined the "diversity of actors" directly involved in network governance concerning police technology (Carboni et al., 2017; Carlsson & Sandström, 2008). In effect, journalists forced transparency that induced policing institutions to respond.

On January 19th, 2020, *New York Times* reporter Kashmir Hill published 'The Secretive Company That Might End Privacy As We Know It,' an extensive profile and exposé on Clearview AI. The article, with its accompanying visual a hypnotic strobing of pictures of everyday people's faces, spotlights how law enforcement in North America had been using Clearview AI's FRT

without disclosing its use to the public. Clearview AI was well-known among police but not among anyone else; Hill's reporting helped expose the company's law enforcement ties while also educating the public about the invasive nature of Clearview's image scraping algorithm. Though Hill's (2020) article focused primarily on law enforcement in the United States, one line near the article's end made offhand mention that, "according to the company and government officials," undisclosed "Canadian law enforcement authorities" are using Clearview, too.

This vague revelation inspired Canadian reporters to investigate Clearview's presence within Canadian policing, though the departments reached for comment denied ever using Clearview at all. On January 21, 2020, *CBC Radio*'s Allie Jaynes published an article titled 'The end of anonymity? Facial recognition app used by police raises serious concerns, say privacy advocates,' in which the TPS explains that they are using facial recognition, but not Clearview AI. David Burke of *CBC News* published a piece on February 10th, 2020, titled 'Use of facial recognition technology by police growing in Canada, as privacy laws lag,' in which the RCMP were quoted as saying that though they "continue to monitor new and evolving technology," facial recognition was not something in their investigative arsenal.

These police departments soon backtracked, admitting their use of the system. After it was reported in *CNET* that Clearview AI had their entire client list stolen in a data breach, it came to light that the TPS, the OPP, and the RCMP were all using Clearview AI (Ng, *CNET,* February 26, 2020). On February 27, 2020, three journalists from *Buzzfeed*—Ryan Mac, Caroline Haskins, and Logan McDonald—published an exposé on Clearview AI, spotlighting the concerning growth of the company's client base across a variety of industries, including the North American criminal justice systems. According to Buzzfeed's reporting, "Clearview's software…has been used by people in more than 2,200 law enforcement departments, government agencies, and companies across 27 countries," with Canada comprising Clearview's largest market outside of the United States (Mac, Haskins & McDonald, February 27, 2020). Among the more than 30 law enforcement agencies in Canada caught using the software, the article singled out the RCMP, "which is listed as a paying customer according to [company logs]," and the TPS, "which despite being on free trials have run more than 3,400 searches across about 150 accounts" (Mac, Haskins & McDonald, Feb. 27, 2020). In sum, it was investigative journalism that dragged Clearview AI out of the shadows in North America, revealing the otherwise undisclosed scope of its use in Canadian policing. What is more, this reporting shed light on inconsistent assessment, communication, and

transparency practices within policing regarding their use of technology, as the RCMP and TPS had only one month prior denied their use of Clearview AI's FRT.[9]

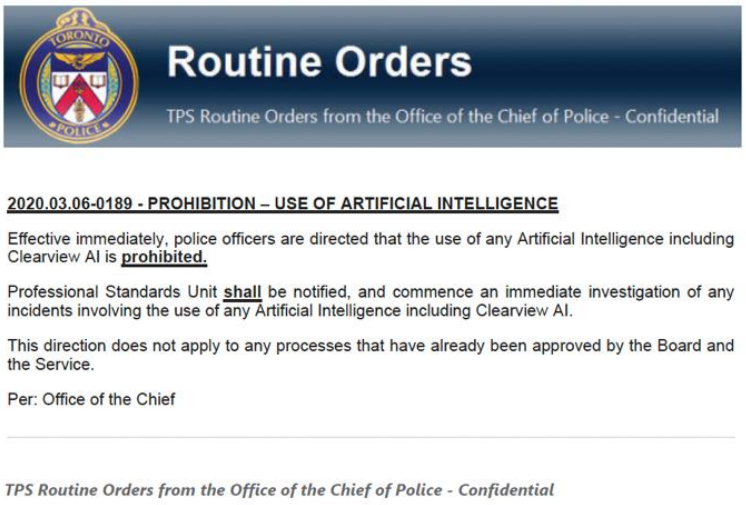
Reporters covering Clearview AI highlighted other existing weaknesses in the governance of police technology, namely loopholes in acquisition and a lack of standardization in approval. Through investigation, Nicole Brockbank of the *CBC* was able to trace most of Clearview's controversial surfacing in Canadian law enforcement to a single point of origin: an otherwise unnamed "victim identification conference in the Netherlands" in 2019 (Brockbank, *CBC*, December 23, 2021).[10] At this conference, Clearview AI gave free trials of its software to police administrators and investigators in attendance. Reporters like Brockbank emphasized the idea that using Clearview AI as a free trial often meant using the tool without proper oversight, and that Clearview AI could be used by police officers without a sign-off from supervisors.

Various units within the Toronto Police Service (TPS) acquired Clearview AI as a "free trial" and used it without prior knowledge or approval of top brass. According to TPS' internal reports, the use of Clearview originated with TPS officers in Child Exploitation Services (CES), before propagating around to other units such as Homicide and Financial Crimes units. Clearview AI spread around the TPS *without the awareness* of then TPS Chief Mark Saunders. Saunders supposedly did not even know about the unregulated use of FRT in his own police force until the Clearview AI controversy was reported in news media. As I uncovered in an FOI disclosure from the TPS, upon learning of Clearview AI's presence within the TPS on February 5th, Saunders issued an immediate Cease & Desist order to all current TPS users of Clearview AI and initiated an internal investigation into the tool. One month later, Saunders issued a Routine Order (see Figure 1) prohibiting the use of all AI in the TPS, including Clearview AI's FRT. The role of investigative journalism cannot be understated here: it was Canadian reporting on Clearview AI that identified the use of Clearview AI in particular police departments, and it was this reporting

[9] Lost in the revelations was the discovery that members of the Ontario Provincial Police had been using Clearview AI's FR tool, too (Breen, *Global News*, March 1, 2020). Somehow, this did not seem to raise as much concern, and to date, the OPP has—at least publicly—not used the controversy to mount AI-related reforms.

[10] This date range suggests that the conference was the "International conference on online investigations: Darknet and online sexual violence against children," held from September 30th to October 1st, 2019, in The Hague, Netherlands (Outline, *Eurojust*, September 29, 2019). This conference was organized in a collaboration between the Council of Europe, an international human rights organization, as well as Eurojust, the European Union Agency for Criminal Justice Cooperation, an associational hub for law enforcement agencies in Europe to cooperate on cross-national crime (Eurojust, n.d.).

that identified to police administrators the lack of administrative sign-off for free trials as a regulatory gap to be filled.



Routine Orders

TPS Routine Orders from the Office of the Chief of Police - Confidential

2020.03.06-0189 - PROHIBITION – USE OF ARTIFICIAL INTELLIGENCE

Effective immediately, police officers are directed that the use of any Artificial Intelligence including Clearview AI is **prohibited.**

Professional Standards Unit **shall** be notified, and commence an immediate investigation of any incidents involving the use of any Artificial Intelligence including Clearview AI.

This direction does not apply to any processes that have already been approved by the Board and the Service.

Per: Office of the Chief

TPS Routine Orders from the Office of the Chief of Police - Confidential

Figure 1: Routine Order from the Office of the Chief

The above example thus highlights the importance of investigative journalism around Clearview AI in contributing to and catalyzing the governance of police technology. This reporting contributes to governance by rendering police technology transparent and holding police accountable for technology's misuse. This reporting was, as I learned in interviews and document analysis, a major catalyst in triggering reform to how FRT, AI, and emerging technologies are governed in policing. The centrality of reporting on Clearview AI suggests that discussions of governance networks around Clearview should embrace Cheng (2019) and Wang, Qi & Ran's (2022) call for expanding analyses of network governance to embrace a wider array of non-governmental actors. By looking at governance reforms mounted by the TPSB and TPS, Canada's privacy commissioners, and the RCMP, it is possible to situate investigate journalists covering Clearview AI as consequential actors *within governance networks* whose role is defined by how their reporting 'shares' resources and information to regulatory actors (Conner, 2016; Thomson & Perry, 2006).

Police in Canada and the world over use technology with a level of secrecy and opacity that few other organizations do, and journalists emerge as one of the primary mechanisms through which actors and groups learn about police technology in the first place. Aside from researchers, journalists reporting on police technology are often the ones excavating information about police

technology initiatives that would otherwise be withheld from the public record, usually by navigating police departments' Freedom of Information (FOI) regimes. Take, for example, Bryan Carney, reporting from *The Tyee,* who reported on documents obtained under an FOI request which shows an RCMP employee signed a "Requisition for goods, services and construction" form to fund a one-year contract with Clearview AI beginning on October 29th, 2019, as well as an invoice from Clearview AI signed by the RCMP on November 26th, 2019 (Carney, *The Tyee*, April 16, 2020). Many of the security, law enforcement, and technology reporters with whom I spoke stressed their role, first and foremost, as regular civilians who just have more time on their hands to interact with FOI offices and sort through the document disclosures these FOI requests occasionally yield.

It is also the job of reporters to translate technological issues into articles, finding the most coherent and precise way to convey stories about oftentimes complex technologies and policies to publics. These journalists often described themselves as a "translator" or "interpreter" for the public, distilling complex technological issues and putting them in sharper, more granular focus, rendering these issues palpable for wider consumption. This is seen throughout the bulk of the Canadian reporting on the police's use of Clearview, which established the baseline set of facts around the controversy with clarity.[11] These articles surfaced otherwise secret information about which departments were using Clearview AI's FRT and to what extent and how Clearview had made its way into Canadian policing, and helped distill for others the key concerns at the controversy's core: the non-consensual collection of photos that makes up Clearview AI's database, the gravity of such privacy violations to the Canadian public, the surreptitious use of such a technology by law enforcement, and the attempts by police to cover up Clearview's use.

Ultimately, this reporting served as the basis for efforts to reform the governance of police technology in Canada, highlighting the important place of journalists within existent and emerging governance networks. When I asked directly about how the Board's AI Policy first came to be, an

[11] For example, it was reporting from Kate Allen and Alex Boutilier of the *Toronto Star* that first highlighted Clearview AI's prevalence in Toronto (February 27, 2020), and Wendy Gillis of the *Toronto Star* who reported on Clearview AI's use by the OPP (March 1, 2020). Wendy Gillis of the *Toronto Star* that found that 144 officers from the TPS conducted over 2800 searches using Clearview AI, and that the RCMP conducted "hundreds of searches…via at least 19 accounts" at the RCMP (Gillis, *Toronto Star,* February 28, 2022; OPC, "Police Use of Technology," 2021, para. 5). And it was Nicole Brockbank of the *CBC* that unearthed an internal TPS report via FOI that revealed just how insular the TPS' use of Clearview was, finding that the TPS started using Clearview's free trial to advance criminal investigations "without consulting anyone other than the company itself and internal supervisors about the legality and accuracy of the technology" (Brockbank, *CBC,* December 23, 2021).

individual from the TPSB who helped create the Policy told me that the reporting on Clearview AI was an incontestable part of the Policy's narrative. This reporting, I was told, helped reveal missing internal governance processes around how technologies are acquired, implemented, and evaluated within the TPS. To quote this individual:

> "**So, yeah, it's true that [Clearview] was the beginning point, and we want to make sure from the start that this sort of thing doesn't happen again.** So that gave us the idea of what this policy is about, and that's **making sure that adopting new technologies, new AI technologies, is going to be going through a process, so everybody knows what it is and nobody just picks up a new technology at a convention and just starts using it without going through the process which is what happened with Clearview**… And all of it was done pretty much as, you know, kind of an 'unauthorized pilot.' **But because there was no process, there was nothing telling them not to. And that's exactly what we want to do to prevent with this policy.** So we started from that point, and that's like, section one. And from there on, okay, so they have to get approval: What's the process?"

Similarly, an individual with one of the TPS's technology-related units involved in developing the TPS' AI Procedure assured me that the Procedure and its governing Policy were specifically designed to address the regulatory gaps highlighted by Canadian reporting on Clearview AI. This reporting, I was told, highlighted to police in Toronto that Clearview the company as well as its FRT was "sketchy as hell," suggesting that the privacy-invasive nature of the tool and the secretive nature of the company were red flags that should have otherwise been caught. This individual further acknowledged that the public and journalistic "uproar" around TPS' use of Clearview stemmed in part from the free trial model on which Clearview entered the TPS, as journalists identified that "it wasn't formal procurement." By sharing information about police flouting specific formal acquisition processes, journalists were able to spur the TPS and TPSB into establishing proper governance processes for responsible and above-board technological acquisition.

Journalistic coverage of Clearview AI was similarly instrumental in inspiring Canada's privacy commissioners—the provincial, territorial, and federal governmental actors responsible for overseeing compliance with public and private sector privacy legislation—with launching investigations into Clearview AI the company and the RCMP. This reporting was also instrumental in the privacy commissioners' creation of two governance documents: guidance for police in Canada using FRT, and a recommended legal framework for governing FRT in Canada. Speaking

with two separate representatives from provincial privacy commissioner offices, I was told by these representatives that they considered Canadian journalists' reporting on Clearview AI as a "trigger point" which "led us to follow up on the matter." A more direct trigger point for privacy commissioners' investigations and governance initiatives was a letter from Charlie Angus, the federal Member of Parliament for the riding of Timmins-James Bay in Ontario, Canada. On Monday, January 27th, 2020, Angus issued a public letter to Daniel Therrien, then Canada's federal privacy commissioner, expressing his concern about "recent media reports" indicating that police forces across North America were using Clearview AI's FRT (Angus, "Re: Possible Use of Facial Recognition Technology," January 27th, 2020). Angus' letter pointed to journalists' reporting on the web-scraping method Clearview AI used to build its image database, highlighting in his letter that he found the potential for Clearview AI to obtain access to Canadians' personal information without their consent "deeply disturbing" (ibid.). Between mounting journalistic coverage and Angus' letter (which itself cites North American journalism on Clearview), the Office of the Privacy Commissioner of Canada (OPC) launched separate investigations into Clearview AI's business practices and into the RCMP's use of Clearview, culminating in findings that both Clearview AI and the RCMP were in violation of Canada's *Privacy Act*, and leading to their creation of privacy guidance and a recommended legal framework for the governance of FRT. The governance network here is complex, involving interface between public actors in Parliament, privacy offices, and policing, as well as the private sector in Clearview as a company, but this interface is bound by the journalists whose work surfaced the troublesome affordances of Clearview AI's FRT (Edelenbos, van Schien & Gerrits, 2010).

Journalism on Clearview AI also influenced the RCMP's efforts to create the National Technology Onboarding Program (NTOP), since reporting on Clearview revealed to the RCMP their lack of a centralized system for evaluating technologies that passed through department thresholds. Slide decks from as early as September 5th, 2020, identify Clearview AI and its media coverage as their "primary program driver." The presentation then includes a slide titled "What happened?" with a screenshot of a Catharine Tunney article from *CBC* headlined "RCMP denied using facial recognition technology – then said it had been using it for months." The next slide reveals that reporting on Clearview AI highlighted an internal "blind spot": that the "RCMP lacks a centralized system that allows for identifying, assessing and tracking new and emerging technologies" (A0764529, pp. 6-7) (Figure 2). An RCMP member responsible for developing

NTOP drew a similar causal connection, citing reporting on the Clearview controversy and its exposure of RCMP's lack of centralized technological onboarding as a direct influence on NTOP's origins:

> "So when Clearview hit the organization, as you know, 'Why did you use this tool?' It really prompted the organization to say 'Are we evaluating technology properly? Do we have the right tools, mechanisms, governance in place to make sure that tools are being used responsibly? And really, do we even know which tools we are using,' right? Because, you know, the organization is big—we work in a distributed environment. So it really afforded us the opportunity to step back and say, 'Let's review what we're doing this organization with these types of tools,' and hence NTOP was born. So when, really, the Clearview issue hit, the RCMP was very much in a reactive mode: How do we deal with this? How do we look at the situation? We looked at it saying 'There are ways to manage this properly.' **So Clearview just really exposed a vulnerability that we had: that we weren't evaluating technology properly**."

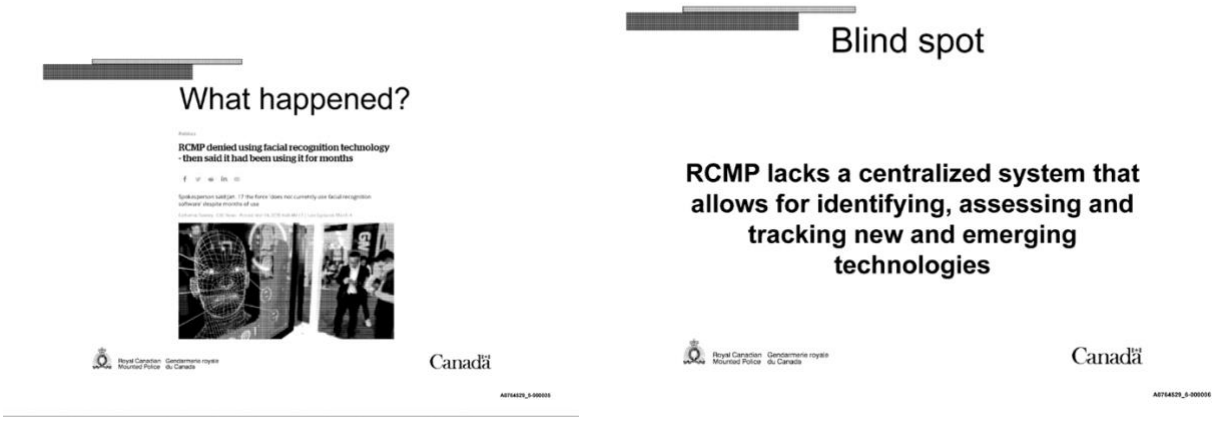

What happened?
RCMP denied using facial recognition technology - then said it had been using it for months
Blind spot
RCMP lacks a centralized system that allows for identifying, assessing and tracking new and emerging technologies

Figure 2: Slides from deck re: journalistic coverage of Clearview AI controversy inspiring creation of NTOP.

Journalists were thus not only significant engines of transparency but also essential "collaborators" through information-sharing and knowledge transmission (Gash, 2022; Gerlak & Heikkila, 2006). As was the case with reporting on Clearview AI, journalists shared information with police departments and government institutions that police and government actors may not have known themselves, surfacing regulatory gaps and privacy-invasive practices that helped institutional actors start bringing police technology under more meaningful control.

When asked about the place of journalists within the governance of police technology, the reporters with whom I spoke for this project recognized their position as *within* a broader

governance network, performing an important role in rendering transparent unaccountable police processes. These journalists also recognized their influence at the *beginning* of a causal chain, as a group whose work inspired others in power to angle for reform. “Who knows what would have happened if I hadn’t done that,” said one journalist involved in early reporting on Clearview AI’s presence in Canada. Kashmir Hill’s *NYT* reporting on Clearview inspired Canadian journalists to dig deeper, but it was the Canadian reporting on Clearview, according to another journalist in our conversations, that really “kicked it off and sort of put it in a new orbit.” Another Canadian journalist writing for a municipal newspaper emphasized these claims, highlighting the importance of journalism as an exercise in transparency-making, as well as journalism’s role in shaping police reform:

> “**I think it's incredibly important that as the media, we asked about it, put it on the front page, regularly put it on the front page for like several weeks, giving it a profile, right?** To be like 'here's what has happened, here's what's happening in police services across the country, and we didn't even know about this.' **And it sends a message to police services and to police services boards and to privacy watchdogs to basically pay attention and to get out in front of it next time.** The Toronto Police had to send out a notice to their officers, if I'm not mistaken, saying 'You can't use tools or software that haven't already been approved or had a policy or whatever,' and that seems again, so self-evident, but I think that helped. **I think our coverage basically generated that**. So I think we are a pretty big part of that.”

Media revelations about Clearview AI thus put regulatory wheels in motion. Journalists shed light on an opaque process of technological acquisition, exposing the non-existent safeguards around a privacy-invasive FRT and police’s dishonesty around the technologies in their arsenal. This highlights the importance of journalists as important stakeholders in sociotechnical debates in policing, and underlines how essential they can be for collaborative and networked governance processes. The work of certain reporters on the police and technology beat helped bring attention to police’s secretive use of Clearview AI as a problem worth addressing, and the problems it revealed with technological transparency and oversight as gaps in need of filling.

Overall, Clearview AI was simply not on the public’s radar, and it was not until American and Canadian reporters started covering Clearview and getting access to internal police documents that the public knew there was something wrong with the technology and something wrong with how police got it and used it. This reporting was the incitement of a controversy: a disagreement between stakeholder groups, some of whom thought that a powerful and invasive technology

should be used but kept secret, and others who thought such a tool should be brought to light and scrutinized. But most important, it demonstrates a necessary expansion of how we make sense of collaborative and network governance, showing how information-sharing can fit into and give shape to emerging governance initiatives around police technology.

Controversy and Tension within Governance Responses to Clearview AI

On the heels of journalists' reporting on the prevalence of Clearview AI in Canadian law enforcement, institutional actors in Canada used this controversy to establish new governance mechanisms designed to better regulate police's increasing reliance on emerging digital technology. The three major governance reforms that will ground this analysis are, as mentioned, the **TPSB's Use of AI Policy and the TPS' AI Procedure; the RCMP's National Technology Onboarding Program; and Canada's provincial, territorial, and federal joint guidance and open letter on FRT in policing.** Looking at these initiatives through the Clearview AI controversy showcases the diversity in approaches to governing police technology, and surface a diverse set of framings, relationships, and tensions between actors and institutions.

a. The TPSB's Use of AI Policy, and the TPS' AI Procedure

Analyzing the aftermaths of the Clearview AI controversy on Toronto policing institutions offers a window into how reform can be born of crisis. But perhaps most importantly, it provides a look at how controversy is or is not framed in the reform efforts that follow. Privately, these institutions cited the Clearview exposé as the inciting incident for reform, taking ownership of their own position at the controversy's centre. But publicly, Toronto policing institutions used their policies and procedures on AI to perform damage control by portraying themselves as early entrants into important but uncharted regulatory terrain. Both the Toronto Police Services Board (TPSB) and the Toronto Police Service (TPS) used their policies to depict themselves as responsible, forward-thinking institutions and to make the case that new AI technologies could be safely harnessed to improve public safety. However, without explicitly acknowledging the Clearview AI controversy, Toronto policing institutions' AI Policy and Procedure implicitly acknowledge it via reforms that tackle the secrecy and siloed decision-making that plagued Toronto's fateful encounter with Clearview.

The TPSB is responsible for setting goals and overarching policies for the TPS to turn into practice, and is thus the body responsible for creating and overseeing an AI Policy.[12] Entering into development following the Clearview AI controversy and approved by the Board in February 2022, the TPSB's AI Policy was created "to establish Board governance for the consideration of the use of new or enhanced technologies using AI, or of previously approved AI technology that is to be used for a novel purpose or in a novel circumstance" (TPSB, AI Policy, 2022). It aims to do so by establishing an assessment and accountability framework that: 1) considers AI's impact on privacy, rights and dignity of individuals; 2) acknowledges "the need for adoption [of] new AI technologies to be done in a transparent manner; 3) evaluates "possible unintended consequences" of police use of AI "prior to any adoption"; 4) establishes "a requirement for appropriate consultations to precede the procurement and deployment" of high-risk AI tools; 5) establishes "mitigation strategies" that "eliminate" any of AI's "identified unintended negative consequences," and; 6) builds in "a pre- and post-deployment, evidence-based evaluation and re-assessment" of any technology both procured and used (ibid.).

However, the TPSB AI Policy makes no mention of the Clearview AI controversy that brought it into being. Instead, the TPSB attempts to gloss over it, attributing the need for governance not to TPS' own personal responsibility in their informal acquisition and secretive use of Clearview AI's FRT, but rather to the wider lack of AI governance in Canada. The TPSB thus frames the AI Policy as a proactive measure done in response to a broad legislative absence, rather than as a reactive measure to getting caught lying about their use of controversial technology. This is conveyed on the webpage announcing the new AI Policy and calling for public input into its development. Here, the TPSB writes that:

> "There is no legislation currently in Ontario that fully regulates the use of AI technologies, nor are there any comprehensive guidelines. The Board is stepping into this new space in recognition of the importance of governing this field, but also recognizing that a Policy governing AI technology use by the Service will have to itself be innovative." (TPSB, "AI Policy Public Consultation," 2021)

Further, the TPSB uses the AI Policy to counterbalance the journalistic coverage of the Clearview AI that portrayed AI and FRT in a negative light, carefully avoiding mention of FRT while extolling the broader benefits of AI. One way in which the TPSB achieves this is by making general

[12] For a full list of TPSB policies, see: https://www.tpsb.ca/policies-by-laws/board-policies.

reference to all of AI, rather than just the use of AI in policing, and pointing to the duality of AI's benefits and risks. In so doing, the TPSB deflects from Clearview AI's unique harms, advancing the narrative that 'AI is complicated' and thus a tool that should be approached cautiously rather than not at all. Quoting again from the public consultation webpage, the TPSB writes that: "Innovative AI technology promises to streamline, simplify and improve many aspects of modern life, providing efficiencies and cost savings. However, AI technology also carries potential risk to privacy, equality, accountability and fairness" (TPSB, "AI Policy Public Consultation," 2021). Following this passage, the TPSB states, "Therefore, the Board is currently developing a Policy to govern the use of new AI technologies by the Service that will allow the Service to reap the benefits of AI technologies in terms of effective and efficient investigations contributing to positive community safety outcomes, while minimizing the identified risks and ensuring transparency in its use of these technologies" (ibid.). The TPSB's framing here elides the Clearview AI controversy entirely, situating their forthcoming governance policy as stemming from the *general* risks and supposed advantages that AI poses society, rather than stemming from any incident that shall remain nameless.

Similar language appears in the final version of the TPSB's AI Policy, which neglects the Clearview AI controversy while foregrounding the general cost-benefit of AI-driven policing. The TSPB Policy (February 2022) states that AI in general "holds the promise of improving the effectiveness of policing services and increasing public safety in Toronto" while also posing threats to "privacy, rights…, dignity and equality of the individuals affected by them" (ibid.). Still, despite the privacy risks and structural opacity that the Clearview AI controversy highlighted, the AI Policy views these benefits as worth the costs, as the Policy is not so much aimed at keeping controversial technology out, but in ensuring that technologies are still adopted, albeit prudently. To quote the AI Policy, the TPSB conceives of the Policy as positioned at the intersection of providing "effective and accountable policing through the prudent adoption of new technologies," while also "ensuring transparency and making certain that policing is provided in accordance with both the law and the interests of the public, and protects and promotes fundamental rights" (TPSB, AI Policy, 2022). By codifying this language, the TPSB acknowledges but minimizes AI's potential for controversy, instead portraying AI as necessary to effective policing.

Similar framing appears in the TPS' AI Procedure, a governance document designed to describe the operational processes required to implement the TPSB's AI Policy, and "to provide a

framework for the acquisition and use of AI technology, using a measured approach to risk assessment, costs, and benefits related to the use of this technology" (TPS, *AI Procedure*, December 2022). Like the TPSB's Policy, the TPS' draft AI Procedure's public-facing webpage and the Procedure itself neglect to mention the Clearview AI controversy. Like the Policy, the Procedure presents a counternarrative to the Clearview AI controversy, framing police use of AI not as dangerous but as operationally necessary. It also frames AI's benefits to public safety as worth the costs, so long as AI is adopted "prudently." To quote the Procedure, the TPS "is continually seeking to provide *effective policing* through the *prudent adoption* of new technologies while ensuring *transparency, service provision in accordance with legislative requirements and the interests of the community*" (TPS, AI Procedure, December 2022; emphasis added). By linking "effective policing" with "the prudent adoption of new technologies," the TPS papers over the harms that the Clearview AI controversy exposed about AI-driven policing and instead conveys AI as a tool to "maximise [the Service's] ability to protect the public" (TPS, AI Procedure, December 2022).

However, a careful read of the TPSB's AI Policy and the TPS' AI Procedure suggest, albeit implicitly, genuine attempts at patching over some of the frictions and conflicts that the Clearview AI controversy exposed within the TPS. As mentioned, the use of Clearview AI's FRT originated with TPS investigators working child exploitation cases, and the technology ultimately circulated to other units within the TPS without TPS Chief Mark Saunders. In an internal report by the TPS uncovered by *CBC* reporter Nicole Brockbank, it was revealed that units within the TPS, specifically Child Exploitation Services (CES), conceived of Clearview AI's FRT as helpful and beneficial. Before it was prohibited by Chief Saunders via Routine Order, CES investigators viewed Clearview AI as a tool through which "investigations were found to be advanced" and a tool to which "general feedback…as an investigative tool is positive" (TPS Detective Operations, "Clearview AI: Usage, Review & Analysis," March 27, 2020, pp. 11-12). Internal reception to the tool was so positive that once CES showcased Clearview AI's FRT to investigators from Sex Crimes, Homicide, and Financial Crimes at an internal TPS case conference, "accounts registered with Clearview AI Inc. increase[d] significantly" (ibid.). Contrary to network and collaborative governance models that often regard decision-making between heterogeneous actors as premised on deliberation and smooth decision-making, the Clearview AI controversy highlighted a rift *within the TPS* around how to acquire and use technology (Agranoff & McGuire, 2001; Bryson,

Crosby & Stone, 2006; Frederickson et al., 2015; Rhodes, 1996; Wang & Ran, 2021). While internal units at the TPS viewed Clearview as a beneficial investigative tool worth incorporating further into police practices, the Chief's reported unawareness about Clearview's presence within the TPS and the controversy that bloomed around it rendered Clearview as something worth purging from the department. It also highlighted relationships where collaboration perhaps *ought* to have been but were otherwise absent, with the lack of administrative oversight producing a fractured governance relationship between police superiors and the units beneath.

In response to the conflicts that this controversy revealed between distinct police actors and groups within the same institution, as well as the lack of transparency that precluded the TPS' use of Clearview from going public, the TPSB's AI Policy and TPS' AI Procedure features governance requirements that can be interpreted as easing tensions between stakeholders within and beyond the TPS. For one, Section 8 of the TPSB's AI Policy contains a provision requiring the TPS "develop and implement a public engagement strategy" whenever they acquire and implement a new AI technology, in order to "transparently inform the public" of the new technology's use (TPSB, AI Policy, February 2022). Though the TPS has yet to develop or implement public engagement strategies on any of its AI technologies in the two years since this Policy came into effect, the provision is evidently a measure to compensate for the transparency failures that characterized the TPS' secretive use of Clearview AI.

What is more, the TPS' AI Procedure, should it come into effect, would create an Artificial Intelligence Technology Committee (AITC) to review AI tools, and would establish a process for this Committee to triage proposed AI "solutions" through screening, consultation, privacy, and risk assessment, and then ultimately acquisition or rejection (TPS, AI Policy, December 2022). Comprised of representatives from across the TPS—including the Information & Technology Command, Legal Services, Business Relationship Management, and more—the AITC premised on networked collaboration. AITC is designed to build consensus across the many branches of the TPS in assessing and evaluating "the intended benefit that an AI technology will deliver," so that every branch is united in their approval of emerging technology (TPS, AI Procedure, December 2022). But perhaps most importantly, AITC membership includes a representative from the "Office of the Chief," and the final step of the technology review process involves "consultation with the Chief of Police" prior to a technology's approval or rejection (ibid., pp. 2-3). By building frequent touchpoints with the TPS Chief into the governance of emerging AI-driven policing tools,

the TPS' AI Procedure appears to be mending one of the central tensions that defined the Clearview AI controversy in Toronto: ensuring that the TPS' Chief of Police is never kept out of the technological loop ever again.

Overall, the TPSB and TPS' approach to governing AI technology elides any overt mention of the Clearview AI controversy, portraying Toronto police institutions as progressive governors of operationally necessary technology, all while excluding the controversy from the Policy and Procedures' public-facing origin stories. However, the Policy and Procedure both grapple with the stakeholder tensions and regulatory gaps that the Clearview controversy exposed. These documents include provisions and regulations that attempt to tackle the secrecy and siloed decision-making that plagued Toronto's fateful encounter with Clearview. Analyzing the Clearview AI controversy in Toronto thus offers a window into the value of controversy as a framework for understanding governance decisions and how they are framed.

b. Provincial, territorial, and federal joint guidance and open letter on facial recognition in policing

The Clearview AI controversy is also a useful analytical entry point for teasing apart the complexities of how provincial, territorial, and federal privacy commissioners sought to govern FRT. As I will discuss, the privacy commissioners' separate investigations of Clearview AI (the company) and the RCMP were points of tension between the stakeholders involved, as the RCMP and Clearview AI ultimately disagreed with the privacy commissioners' findings and recommendations. This example showcases how controversy can complicate our overlapping conceptions of network and collaborative governance as premised on "coordinating activities," "structures of interdependence," and "achieving collective objectives" (Agranoff & McGuire, 2001; Bryson, Crosby & Stone, 2006; Frederickson et al., 2015; Rhodes, 1996; Wang & Ran, 2021). Further, the Clearview AI controversy shows how stakeholders like privacy commissioners position their governance interventions within an uncertain regulatory space. Of the policy documents that Canada's privacy commissioners ultimately produced, one was designed to steer or guide police away from another Clearview-like controversy and toward compliance with the laws Canada already has, while the other was designed to lay the groundwork for what those laws could be in a post-Clearview world. In so doing, privacy commissioners muddle their own regulatory abilities.

In Canada, privacy commissioners fulfill several functions, many of which fall beyond the ambit of policing. Privacy commissioners oversee institutions and businesses' compliance with privacy law, review responses to Access to Information (ATIP) requests when civilians are unsatisfied, maintain an advocacy position through which they educate the public on privacy-related concerns, and most relevant to the current study, conduct investigations into privacy breaches. Canada has one federal privacy commissioner, the Office of the Privacy Commissioner of Canada (OPC), as well as a privacy office for each province and territory. All privacy commissioners oversee public sector privacy, while the federal commissioner and three provinces—Alberta, Quebec, and British Columbia—maintain a split mandate whereby they oversee private sector privacy legislation, as well. As I learned in conversations with individuals from privacy offices across Canada, differences also exist with respect to these offices' order-making power. Most privacy offices (the federal office included) solely have the authority to make privacy-related *recommendations* to public sector bodies, but have no force of law to back those recommendations up. Notable exceptions to this are, once again, Alberta, Quebec, and British Columbia, the only provinces with authority to make legally binding privacy recommendations. As I will discuss here and in the chapters to follow, some privacy commissioners' inability to make and enforce legally binding decisions has created problems for effectively regulating FRT and AI in Canadian policing.

In February 2020, on the heels of media reports about Clearview AI's presence in Canada and the urgings of Members of Parliament (MPs), the federal privacy commissioner Daniel Therrien announced two separate investigations: a joint investigation between the OPC and the privacy commissioners of British Columbia, Alberta, and Quebec into Clearview AI as a company, and an investigation into the RCMP's use of the controversial AI tool. At the end of their investigation into Clearview AI, the OPC and the three provincial privacy commissioners found that the company had violated private sector privacy laws on the federal and provincial levels by collecting, using, and disclosing personal biometric information without requisite consent (PIPEDA Findings #2021-001, February 2, 2021, para. 18). Similarly, the OPC's investigation of the RCMP's use of Clearview AI's FRT found that the RCMP 's use of the troublesome tech contravened Canada's federal public sector privacy legislation, the *Privacy Act.* According to the report, "the RCMP failed to properly assess the potential Privacy Act compliance risks" (OPC, "Police use of Facial Recognition Technology in Canada and the way forward," paras. 6 & 27).

Further, the RCMP "did not have systems in place to track, identify, assess, and control such novel collection of personal information," and the RCMP violated the *Act* by "collect[ing] personal information through contracts with a private company that itself collected the personal information unlawfully" (ibid.).

It is not surprising that investigations can be adversarial affairs, but these investigations revealed public-to-private and public-to-public frictions that highlight the limits of privacy commissioners' mandate in regulating police technology (Provan & Kenis, 2008; Yang, 2020). Specifically, after the OPC published its findings of its investigations into Clearview AI and the RCMP and issued them recommendations for remedy, both Clearview AI and the RCMP separately *disagreed* with the privacy commissioners' findings and recommendations. According to the OPC, Clearview disagreed with the privacy commissioners' findings that the company had contravened myriad provincial and federal privacy laws, saying that their practices were legal because images of people's faces were taken from the open web—what Clearview lawyer Tom Ekeland referred to as "publicly available data from the public internet" (Boutilier & Gillis, *Toronto Star*, July 6, 2020). Further, Clearview AI alleged that the company's web-scraping activities did not cause any harm to individuals, threatened Canada's privacy commissioners that they should suspend their investigation, and refused to commit to following any of the privacy offices' recommendations (PIPEDA Findings #2021-001, February 2, 2021, paras. 113-117). On July 6, 2020, amid the investigation, Clearview AI withdrew its services from the Canadian market but refused, despite privacy commissioners' recommendations and orders, to delete the images of Canadians Clearview had already collected, and refused to cease collecting Canadians' personal information (OPC, 'News Release,' July 6, 2020). This result is a curious by-product of collaborative and network governance that points to privacy commissioners' inconsistent regulatory power: though Canada's privacy commissioners were not actually able to work collaboratively with Clearview AI on governing the company's privacy-invasive practices, their investigation nevertheless managed to achieve a regulatory effect by leading to Clearview AI withdrawing their illegal services from Canada.

The OPC's investigation into the RCMP yielded similar results, highlighting frictions between the OPC and RCMP as stakeholders that nevertheless culminated in commitments to collaborative governance. Following the OPC's investigation into the RCMP's use of Clearview AI, the RCMP issued a response acknowledging the legitimacy of the process through which the

OPC had generated its findings and agreed to heed the OPC's recommendations for rectifying their violation of the *Privacy Act*. But in private, the RCMP, much like Clearview, very much disagreed with the OPC's findings. In a statement meant to publicly acknowledge the legitimacy of the OPC's investigation, the RCMP pledged to improve their procedures, policies, and training around "assessing new and emerging technologies" (RCMP, "Response to Report," June 10, 2021). However, speaking notes attached to a slide deck found within the FOI disclosure I received from the RCMP suggested that the results of this investigation were a point of contention. As part of a presentation titled "OPC Investigation into RCMP Use of Clearview AI Facial Recognition: Presentation to the Operations Committee, October 12, 2021," the presenter's speaking notes show that, based on conversations had with the RCMP's Legal Services Unit and Department of Justice privacy law officials:

> "…we disagreed that the RCMP was in violation of the *Privacy Act* as it did not seem that the OPC had substantiated the finding that the RCMP was not within its authority to collect personal information. Nor does the *Privacy Act* expressly impose a duty on the RCMP to examine the collection authority of a non-governmental third party to ensure compliance with PIPEDA or the *Privacy Act*." (A0764529, p. 137).

Still, despite the disagreement, the RCMP heeded the OPC's recommendations, once again highlighting privacy commissioners' bizarre and paradoxical regulatory effects in the wake of Clearview AI. Privacy commissioners are still able to get the result they want—the establishment of post-Clearview governance on police technology—despite stakeholders' abilities to exist in friction with them and even reject their legal findings as erroneous and non-binding.

On top of motivating investigations, the Clearview AI controversy catalyzed Canada's joint privacy commissioners into developing and releasing two governance artifacts. These documents are critical of AI, FRT, and the regulatory vacuum in which they operate, but they also exist in tension with one another, gesturing toward privacy commissioners' ambivalent positioning and weak enforcement powers. In May 2022, a year after publishing the findings of their investigations into Clearview and the RCMP, Canada's provincial, territorial, and federal privacy commissioners released joint guidance on facial recognition in policing. Though neither legally binding nor "opining on the legality of specific uses of FR[T] by police," the joint guidance was designed to "clarify police agencies' privacy obligations relating to the use of FR[T] under current laws, with a view to helping ensure that any use of the technology complies with the law, minimizes privacy risks, and respects privacy rights" (OPC, "Police Use of FRT in Canada," June 10, 2021). The

guidance emerged out of what privacy commissioners had already identified as a much bigger problem they had unearthed in their prior investigations: that "unlike other forms of biometrics collected by law enforcement, facial recognition is not subject to a clear and comprehensive set of rules" (ibid.). "Its use," the report continued, "is regulated through a patchwork of statutes and case law that, for the most part, do not specifically address the risks posed by the technology" (ibid.).[13] "Canada's federal, provincial, and territorial privacy commissioners are of the opinion," this guidance begins, "that the current legislative context for police use of FR is insufficient," which has created "significant uncertainty about the circumstances in which FR use by police is lawful" (OPC, 2022, paras. 2-4). It is "in the absence of a comprehensive legal framework" that this guidance exists, for the purpose of "clarify[ing] police agencies' privacy obligations relating to the use of FR under current laws" (OPC, 2022, para. 4). Though this guidance is critical of inadequate regulatory regimes, the guidance is also flawed: it critiques the patchiness of the wider governance network in which FRT operates, but essentially permits use of a technology that privacy commissioners had already deemed controversial and illegal—so long as it is used well.

The guidance is thrown into further tension by the privacy commissioners' recommended legal framework document. Released in tandem, both documents at once reinforce *and* undercut each other's regulatory power. For one, the recommended legal framework document reinforces the guidance's message by reiterating the regulatory gaps around police technology. The recommended framework and guidance documents use similar language to convey this, emphasizing the "patchwork of statutes" and the lack of a "clear and comprehensive set of rules" governing police use of FRT in Canada (OPC et al., "Joint Statement," May 2, 2022). However, the recommended legal framework document undercuts the guidance's regulatory potential, referring to the guidance as an "interim measure" that "is not sufficient to address the challenges posed by police use of FR[T]" (ibid.).

[13] For example, the privacy guidance draws on the *Canadian Charter of Rights and Freedoms* and relevant Charter jurisprudence; Canada's federal *Privacy Act*; Section 487.01 of the *Criminal Code of Canada,* which "provides for warrants that permit intrusion on individuals' privacy when a judge is satisfied that there are reasonable grounds to believe that an offence has been or will be committed and that information concerning the offence will be obtained through the use of the technique or device" (OPC, 2022, para. 44); the *Identification of Criminals Act*, which "allows police agencies to fingerprint or photograph individuals charged with, or convicted of, certain crimes for the purposes of identification" (OPC, 2022, para. 45); as well as common law tests for police powers—a test which "requires a police action be 'reasonably necessary' for the fulfillment of the police duty, which in turn requires weighing the importance of the performance of the duty against the extent of the interference with the liberty interest in question" (OPC, 2022, footnote 26).

Further tensions arise when these documents are considered alongside the findings from the privacy commissioners' investigations into Clearview AI and the RCMP mentioned above. From their investigations, Canada's privacy commissioners' findings suggested that Canadian privacy law was strong enough for privacy commissioners to capture the RCMP and Clearview AI's privacy violations. However, the guidance and recommended legal framework documents undermine those investigative findings, suggesting that that same privacy law is by and large "insufficient" to properly regulate FRT (ibid.).

And while the privacy commissioners' guidance document suggests that Canada's regulatory regime around police use of FRT is inadequate but workable, the recommended framework does not. Instead, this document argues for a new legal framework that explicitly delineates acceptable and unacceptable applications of FRT in policing (ibid.). From the investigations into Clearview and the RCMP, Canada's privacy commissioners' findings stated that Canada's biggest privacy law was more than sufficient to capture a malicious private actor and a woefully reckless police department, but the privacy commissioners' guidance and recommended legal frameworks paint the law as-is as insufficient for governing police use of FRT. This tension creates more confusion than it solves, with the OPC portraying Canadian privacy law as adequate and inadequate at the same time.

What is more, the privacy commissioners' recommended legal framework document reinforces privacy commissioners' regulatory limitations by viewing police use of FRT almost exclusively as a privacy issue. Privacy is, of course, a key issue in the Clearview AI controversy, and the recommended legal framework provides for provisions that seek to patch the specific regulatory gaps that the Clearview AI controversy exposed. This includes creating robust privacy protections specific to FRT and providing "clear and explicit restrictions against certain uses…of FR[T] that could have indefensible effects on privacy" (OPC et al., "Joint Statement," May 2, 2022).

However, by focusing on specific privacy-invasive "uses" of FRT, the recommended legal framework fails to capture how police come to acquire privacy-invasive FRT in the first place. What is more, the framework even filters technological transparency through a privacy lens, highlighting that "strong transparency measures are needed…to ensure individuals have an opportunity to be informed about what personal information may be collected about them, and how it may be used" (ibid.). This is important, but it only captures one part of the Clearview AI

controversy (the company's web scraping practices) and not the other (the police's secretive use of FRT and ability to test technology without oversight). It is not surprising that a legal framework proposed by privacy commissioners puts privacy first, but proposing a privacy-centric legal framework for police use of FRT neglects other relevant considerations such as the technology's tendency for bias and police's tendency to procure technology with limited oversight.

In sum, the Clearview AI controversy brought to privacy commissioners' attention a troublesome technology requiring further investigation. The investigations that followed highlighted the RCMP and Clearview AI's violations of Canada's *Privacy Act*, while highlighting broader gaps in how police technology is governed. Further, these investigations inspired Canada's privacy commissioners to create guidance and a recommended legal framework, designed to at once plug holes in Canada's existing privacy patchwork while signalling that this patchwork is legally ambiguous and in need of complete and utter overhaul. However, when taken together, the privacy commissioners' investigations, guidance, and recommended legal framework exist in conflict with one another. The tensions between these investigations and documents muddle privacy commissioners' regulatory abilities and show an institution flattening a complex technological controversy into a singular privacy issue.

c. The RCMP's National Technology Onboarding Program

The RCMP's response to the Clearview AI controversy stands in contrast to the governance initiatives of Toronto's policing institutions and Canada's provincial, territorial, and privacy commissioners. The governance initiative that emerged from the RCMP's use of Clearview AI—the National Technology Onboarding Program, or NTOP—highlights an RCMP reckoning with its responsibility in the controversy. It also shows an agency looking inward at its own structural weaknesses rather than outward at the patchy legislative landscape that many stakeholders said made the Clearview AI controversy possible. I show that the decentralization of internal systems that the Clearview AI controversy exposed pushed the RCMP toward developing an insular a governance structure that surfaced conflicts between the RCMP and external stakeholders.

By contrast to Toronto policing institutions efforts to hide the importance of the Clearview AI controversy to proposed reforms, the RCMP's public and private narratives cite NTOP as emerging directly from the Clearview exposé. In March 2021, following their investigation that found the RCMP's use of Clearview AI in violation of the *Privacy Act*, the OPC issued a set of

recommendations to the RCMP which included "conducting thorough assessments, creating procedures and systems to track the use of technologies that collect personal information and training to ensure decision-makers understand the limitations of collection under the *Privacy Act*" (A0764529, p. 156, slide deck from September 13th, 2022). Even though the establishment of NTOP was already underway by the time the OPC issued their recommendations, then RCMP Commissioner Brenda Lucki committed to meeting them, pledging to improve RCMP procedures, policies, and training around assessing and implementing new technologies by mounting a more centralized initiative for streamlining all things technological (ibid.).

The reason that the development of NTOP was already well underway by the time the privacy commissioners issued their findings was because the RCMP did not necessarily need the privacy commissioners' investigations to tell them where they were at fault. In fact, the RCMP had already reflected on it themselves, and were very open about their failures in the wake of the Clearview AI controversy. In a conference presentation on efforts by Canadian police to govern AI, a representative from NTOP quipped that the Clearview AI controversy taught them that "officers are crafty" at bringing technology into the RCMP. The NTOP representative soon shifted the blame from individual officers to RCMP-wide structures, clarifying that what the Clearview AI controversy revealed was that the RCMP was "very decentralized in the way we run technology." "Even though [the RCMP] have a CIO (Chief Information Officer)," said the representative, the existent RCMP systems were not enough to govern emerging technology.

NTOP was explicitly created to address this "blind spot" of decentralization (Figure 2). According to a "Framework Proposal" contained on a slide deck dated September 25th, 2020, and disclosed to me via FOI, the RCMP sought to address this blind spot through a six-prong mandate for NTOP (emphasis included): "1. Respond to investigational needs through **innovation or procurement;** 2. Leverage internal technology experts and establish a standard **evaluation** framework; 3. Develop appropriate **policy, legal and privacy** frameworks; 4. Work with internal business lines to identify, assess, document, and safely **deploy** new tools and techniques; 5. **Track** the tool/technology through management of a centralized inventory; and, 6. Be **transparent** where possible" (ATIP Release Package #A202205007, p. 7, emphasis included).

The RCMP's technological decentralization predating NTOP cannot be overstated. As I learned from conversations with members from the RCMP, technological initiatives at the RCMP before NTOP could fall under a number of different sub-units and departments, each with their

own mandates and purviews. These include the RCMP's Action, Innovation, and Modernization (AIM) unit, their Data and Analytics program, the Information Management and Information Technology (IM/IT) program, the Technical Operations team and the Strategic Services Branch that provides Technical Operations with support, as well as Technical Investigation Services. There was also the RCMP's Technical Case Management program, an offshoot of Technical Investigation Services established in 2018 to provide technical advice and case management to "identify the appropriate technical capabilities required to satisfy investigative objectives" (Blair, "Departmental Results Report," 2019). NTOP began as an offshoot of Technical Operations and Technical Case Management, but expanded to link pre-existing units and departments together whose mandates pertain to technology, and centralize an otherwise disordered regulatory regime (RCMP, "Response to the Report," June 10, 2021).

Through NTOP, the RCMP was able to make good on the lessons of Clearview AI by centralizing technological decision-making. NTOP thus emerged as a governance network comprised of interlocking groups and actors internal to the RCMP. NTOP folds in the RCMP's Access to Information and Privacy (ATIP) branch for *Privacy Act* compliance and disclosures about technology; Legal Services Unit (LSU) to ensure the proposed technology is compliant with the *Charter* "and other applicable laws and regulations"; and close collaboration with the Action, Innovation and Modernization (AIM) office to provide regulatory analysis and correction when "any aspect of the [proposed technological] capability (such as deployment, training, or policies) may create barriers to equity, diversity, or inclusion" (A0764529, pp. 68). By bringing varying RCMP units together under the NTOP banner, NTOP emerges as something of a collaborative governance network, with different units contributing different areas of speciality to the overall governance of police technology in the force.

Looking to NTOP may highlight the RCMP's capacity for internal collaboration, but simultaneously highlights the challenges RCMP faces in collaborating with those outside the organization. Specifically, internal RCMP documents show how the development of NTOP was built on further conflicts between the RCMP and the OPC in the wake of the Clearview AI controversy. In the speaking notes for the slide deck mentioned above, an RCMP presenter states that "we may not have agreed with the findings [of the OPC's investigation into the RCMP's use of Clearview AI], but we do recognize the need for change and to do better" (A0764529, p. 139). Still, the presenter refers to the timeline on which the OPC has put the RCMP to implement these

recommendations as "aggressive," and that this aggressive timeline has created "pressures" that conflict with the "need to ensure that we properly identify gaps and issues," creating "a delta between OPC expectations and getting it right" (A0764529, pp. 139, 143). In other words, the OPC's external demands can potentially jeopardize the quality of governance that may emerge from the RCMP on the heels of the OPC's recommendations. "The OPC," the presenter adds, "expects that the RCMP takes full action and have indicated that they will be vocal if we do not," betraying a hint of resentment at what appears to be a threat (A0764529, p. 140). At a certain point in the presentation, the presenter stops referring to the OPC's recommendations as such, referring to them instead as "criticisms"—suggesting an association between the two rooted within conflict (A0764529, p. 142). Overall, the RCMP's ability to establish a technological governance program despite clashing with the OPC and its recommendations further validates this project's network governance framing, showing how stakeholders navigate conflict and unequal power dynamics to achieve governance goals (Cleveland, 1972; Hermansson, 2016; Purdy, 2012; Ran & Qi, 2019).

However, the centralization of technological governance under the NTOP banner has made NTOP rather insular. As a result, NTOP's increased insularity has reduced (or at least has not improved) transparency around police technology in the RCMP. The Clearview AI controversy exposed a dearth in RCMP transparency mechanisms around technology. NTOP's Program Charter states that the RCMP's lack of transparency about their use of Clearview AI, as well as being caught in a media-publicized lie about its use, "severely impacted public trust" (p. 52 of FOI document). The controversy placed a renewed importance on openness with the public about the use of technology, as "very few members of the public understand how policing operations work which creates fear of the unknown. By being transparent about what capabilities are being used and how they work," this Charter says, "people become less afraid which in turn re-instill trust in the RCMP" (p. 27 of FOI document).

To remedy this, NTOP was built to include a Transparency and Outreach Team, designed to "identify best practices for transparency as it relates to specific technology-based capabilities," "establish and maintain close working relationships with public stakeholders," "conduct proactive outreach in order to establish public trust and foster transparency," "coordinate the release of information, including transparency reports, in collaboration with ATIP, to respond to requests from both RCMP partners and the public," and "Communicate with NTOP clients regarding their responsibilities before, during, and after the NTOP process" (A0764529, p. 20). However, in the

nearly four years since NTOP was first proposed, NTOP has yet to release a transparency report despite their mandate to do so. This further entrenches the transparency failures that the Clearview AI controversy exposed, and highlights that we know as much about which emerging technologies the RCMP is using *now* as we did when the Clearview AI controversy first broke four years ago.

In speaking with a representative from NTOP, I was told that NTOP has a "pretty good internal communications strategy" as part of their Outreach initiative. This initiative is comprised of frequent mailers to staff and a policy available on the RCMP's intranet, suggesting that there are rigorous *internal* efforts to ensure technologies enter the NTOP pipeline, but few efforts to circulate information about technology externally. Interestingly, this individual explained that the lack of *external* outreach is, in part, because of how successful NTOP has been at *internal* outreach: according to this individual, NTOP is "still trying to figure out how to effectively and efficiently do the assessments" amid an influx of NTOP applications from units within the RCMP. This individual added that until NTOP reaches a point where they are "confident" in the quality of their assessments, "and that they're sufficiently comprehensive and we are able to *explain* the process and explain the tools and technologies in an appropriate way to the public," only then will they circulate information about technology to the public. NTOP appears to be a victim of their own success, bogged down by so much uptake on their centralized system that they cannot keep up with transparency requirements.

Overall, the Clearview AI controversy provided two relevant interest groups a window into separate regulatory gaps. For one, it gave police, in the form of the RCMP, an understanding of their own shortcomings, spotlighting key "blind spots" that internal and department-wide reform could, ideally, address. Further, it provided privacy commissioners with an opportunity to subject police to investigative scrutiny, which revealed how the use of technology ostensibly violated federal law. Unlike the TPSB and TPS, who gestured toward a broader lack in regulation, the RCMP used the Clearview AI controversy to look inward, point to their own fallibility, and create measures to rectify a problem for which they took responsibility. These measures were perhaps *too* effective, leading to centralization of technological review processes at the expense of outward transparency. Still, the model that NTOP presents is appealing in its collaborative and networked structure that encourages each group within the network to use their expertise toward assessing all angles of prospective police technologies.

Conclusion

To quote a police technology consultant working in Ontario, "Clearview was a different shenanigan." Clearview AI's emergence in the world of police technology offered police something that prior FRT had not: the ability to break beyond the mugshot database and link photos of people to their online profiles. The technology itself, as well as its secretive adoption by police in Canada, proved a source of controversy, and it was up to investigative journalists to highlight this technology's troublesome particulars and the conditions of its use. Ultimately, this reporting and the controversy that ensued was essential in shaping the way police technology was governed.

The police's use of Clearview AI was but one single source of controversy, but its influence was multifold, inspiring numerous stakeholders and spurring them into establishing regulations for FRT and AI in Canadian policing. These governance initiatives—the Toronto policing institutions' development of a policy and a procedure to govern their acquisition and use of AI technologies; Canada's privacy commissioners' investigations into Clearview AI and the RCMP's use of the company's technology, as well as the guidance and a recommended legal framework for how FRT should be governed; and the RCMP's NTOP—were built in direct response to the controversy but took different shapes. Toronto policing institutions used the controversy to build governance that highlighted their role as regulatory innovators creating regulations on shaky regulatory ground, while ensuring that these governance mechanisms addressed the lack of administrative oversight the Clearview AI controversy revealed. Privacy commissioners mirrored Toronto policing institutions' gestures toward broader legislative uncertainty in the governance of police use of technology. However, they undercut their own regulatory efficiency by simultaneously endorsing and decrying FRT, and by simultaneously deeming privacy law both adequate and inadequate for governing FRT's harms. The RCMP, by contrast, used the controversy as an opportunity to look inward, establishing a centralized program for standardizing the governance of police technology. In centralizing technology governance, though, the RCMP has failed to make good on the external stakeholder engagement it envisioned upon NTOP's inception.

Looking at initiatives from these three levels of government highlights the importance of a controversy-centred analysis of police technology. It also highlights the importance of looking at this controversy through collaborative and network governance in order to account for a wider range of police technology stakeholders, and to better explore the friction and disagreement both within these stakeholders and between them. Looking at conflict surfaces the otherwise invisible

groups that hold a stake in police technology issues. Controversy helps spotlight relevant actors and institutions about police technology and helps spotlight where they agree and disagree. Further, controversy can generate insights on how governance initiatives came to be, how they emerging initiatives are positioned as addressing particular governance problems, and how these initiatives are often fraught with tensions of their own. Such was the case with Clearview AI, which served as the gravitational centre around which distinct stakeholders orbited (and continue to orbit). Controversy is also a useful methodological tool, allowing us to observe and describe around sociotechnical issues (Nelkin, 1971; Nelkin, 1974; Venturini, 2010). Controversy not only helps in establishing the many actors and institutions with a stake in police technology. It also helps in teasing out the broken regulatory landscapes which governance reforms seek to repair—the giant spaces where policies and procedures and laws *should* be but are not, the fault lines where good governance slips through. Controversy provides a window into what existing governance mechanisms can be improved and where new governance mechanisms can be slotted in.

But once governance is proposed as a resolution, a new sociotechnical debate opens up: *how* to actually govern police technology. And as we will see in the coming chapter, the *how* is inflected by power asymmetries. Chapter 2 will discuss how police departments and government agencies across Canada mounted collaborative and inclusive initiatives for governing FRT and AI, that remain seriously constrained by their inability to accommodate competing input from government, civil society, private industry, and police stakeholders. Ultimately, governance of police technology is only collaborative in theory; in practice, it remains subject to disagreement, dissensus, and, perhaps above all, power asymmetries that systematically favour police.

Chapter 2: Parsing Gaps and Asymmetries within the Police-Tech-Governance Patchwork

Back in the conference centre ballroom, IACP President Dwight Henninger and IACP Sub-Committee Chair Catherine Miller are presenting the IACP/Oracle Scanlon Excellence in Criminal Justice Information Sharing Award to a chipper middle-aged woman named Bonnie Locke. Bonnie is the Director of Business Development at Nlets, a company that specializes in linking law enforcement telecommunications systems. It does not sound like much, but given the wave of applause she is getting, Bonnie is the rockstar of the police technology world: everyone knows Bonnie, and everyone loves her. Accepting her award, Bonnie hems and haws and thanks the countless folks who have gotten her to where she is, but as Bonnie ends her speech, she abandons all humility to crown herself a royal. "I'm the queen of networking," she declares. "I love to put people in touch." Bonnie links law enforcement systems for a living, but she loves linking *people*, too. "If you want me to introduce you to anyone, come find me," she adds. "I'll make that connection." I spend the rest of the conference trying to wade through the thicket of attendees who stand clustered around Bonnie at all times, desperate to introduce myself, desperate to take her up on her power of connection, but never getting close.

As I slip through the cracks within Bonnie's network of police professionals and technology vendors, I am reminded of a word that had come up time and again in my conversations with individuals from across police technology: *patchwork*. Participants from the world of policing, technology, government, and civil society told me that the diverse collection of actors, institutions, and artifacts swirling around regulatory questions in policing and technology exist in limbo. Governance regimes, they said, were places of legislative ambiguity and policy gaps, uncertain standards, and unenforceable procedures. They added that new mechanisms of regulation were intervening on shaky ground: emerging attempts at governing police technology like FRT, AI, and cutting-edge digital tools were trying to bring coherence and stability to a regulatory space that was cryptic and wobbly at best. The collaborative and productive spirit of networks within police technology, like the one touted by the self-professed "queen of networking" Bonnie Locke, were illusory my participants: the reality was that police technology's governance structures were far patchier than expected.

Few stakeholders ever gave concrete examples of what this patchwork entailed. I had to get to the bottom of what this patchwork actually *was* to understand what laws and policies allowed the Clearview AI controversy to come to be. Uncovering this patchwork was also important for

further comprehending the legal and political backdrop against which police technology debates are situated, and for understanding how stakeholder groups would interact, if at all, with the new governance mechanisms to which I had turned my attention. After all, these new mechanisms—the TPSB's AI Policy and TPS' AI Procedure; the privacy commissioners' joint guidance and recommended legal framework for FRT; and the RCMP's NTOP—were not *replacing* any existing laws; rather, they would be clicking into place alongside other institutions, groups, and their patchworked laws, policies, procedures, and regulations.

In this chapter, I will explore the political and legal landscape of police technology governance, charting and analyzing the patchwork of governance actors and artifacts that not only gave rise to the Clearview AI controversy but that continue to exist in its wake. This chapter builds on the previous chapter by continuing to flesh out the different institutions, laws, and policies that are meant to govern police technology in Canada. However, this chapter will focus on how issues of power and authority complicate traditional understandings of network and collaborative governance. Ultimately, I will argue that existing governance structures, as well as the trio of governance mechanisms explored in the previous chapter, face challenges that restrict and undermine their capacity to meaningfully regulate police technology. This analysis offers a counterpoint to network and collaborative governance scholars' assumptions that actors work through these challenges and tensions collaboratively to produce and sustain strong, smooth ties (Ansell & Gash, 2007; Bryson, Crosby & Stone, 2015; Emerson et al., 2012; Thomson & Perry, 2006; cited in Duijn, Bannink & Ybema, 2021). Instead, I argue that the governance of police technology is frequently stymied by power imbalances between stakeholders and the limits of stakeholders' authority. Governance of police technology, as my informants suggested, looks like a network, but functions much more like a patchwork.

To show this, I will trace regulatory gaps that are both external and internal to policing, charting the legislative conditions that allow police technologies to evade oversight. Second, I will revisit the implications of stakeholder collaboration within and beyond policing, showing how police conduct consultations in a manner which avoids delegating authority to other stakeholders, while showing how police expectations of these consultation exercises vary from the expectations of those who seek to restrict police use of AI-enabled tools. By charting this patchwork, I expose the holes in the quilt that is the governance of police technology, highlighting some of the immobilities, barriers, and uneven flows of power produced by the uneven overlays and absent

intersections between disparate governance regimes. Overall, I argue that police technologies escape regulatory oversight because regulatory regimes are, by and large, structured to favour police institutions.

The False Promise of Governance

a. Regulatory Gaps External to Policing

Police technologies slip through cracks between formalized governance institutions that would otherwise appear to have power to regulate certain aspects of police, technology, or both. This unfolds Across municipal, provincial, and federal levels: institutions abound that *seem* like they would have regulatory authority over how police source, acquire, implement, evaluate, and control technology, but somehow these processes are excluded from an institution's jurisdiction or mandate. Some of these are bodies, institutions, or regulatory artifacts that formally govern police, but somehow not police's *technology*; others are bodies, institutions, or regulatory artifacts that formally govern technology, but not the *police*'s use of it.

Such is the case at the municipal level in Toronto. In conversation with a Toronto City Councillor who is known for being critical of police, I learned that Toronto City Council has *some* regulatory authority over the Toronto policing institutions, but this authority is limited. Toronto City Council's sole function with respect to Toronto policing is what this City Councillor sarcastically referred to as "the fun part": approving the TPSB's annual police budget request. This limited authority, I learned, is a constant source of frustration for certain City Council members hoping to exact more influence over something in need of regulation. It is also a political hot potato. I was told that Councillors hoping to exact greater influence over Toronto policing, such as by questioning line items for technology within the police budget, ultimately risk facing accusations by other Councillors of holding anti-police bias. Though Toronto City Councillors have occasionally been critical of police technology, most notably in the summer of 2018 when the TPSB sough City Council approval for additional funding to procure the automated gunshot detection system ShotSpotter (Janus, 2019), City Councillors otherwise steer clear of dabbling in questions of policing (and police technology) altogether. And while Toronto City Council appoints between two and three councillors to serve on the TPSB (pointing to a networked governance relationship between municipal government and police oversight bodies), I was told that these councillors are usually restricted in how critical they can be of police operations for many of the

same reasons outlined above. This shows how within governance networks, the authority of municipal government can be limited—by virtue of limited mandate or by political pressure— in its capacity to oversee police technology.

The Councillor with whom I spoke pointed to other municipalities in North America to question why Toronto Police's "operating decisions [were] not accountable to Toronto City Council," and wondering why Toronto could not take inspiration from elsewhere. Specifically, this Councillor highlighted the New York City Council (NYCC) as an example of a municipal government that has found a way to regulate police technology. In June of 2020, the NYCC voted overwhelmingly in favour of enacting the Public Oversight of Surveillance Technology (POST) Act (NYCC, "Legislation Details," 2020). The POST Act was enacted to increase transparency and oversight of the New York Police Department's (NYPD) use of surveillance technologies and information sharing networks (ibid.). The Act, as enforced by the NYCC, requires the NYPD to disclose information about the surveillance technologies it currently uses and intends to acquire, as well as the measures the NYPD has put in place to ensure present and future tools protect people's privacy and civil liberties (Brennan Center for Justice, "POST Act," n.d.). I will discuss the POST Act in greater detail later, but it is worth mentioning here to show the unrealized potential in Toronto for involving municipal government in governing police technology.

Similar oversight gaps exist in other municipal institutions that have technology mandates. The City of Toronto's Technology Services Division (TSD), for example, is tasked with overseeing investments into and management of digital transformation across the City's public services. But in reviewing the TSD's 2023 operating budget, it became clear that the TSD's technological steering and oversight applies to all aspects of City services *but not policing*. Further analysis of TSD's budget and brief correspondence with a representative from TSD suggests that the Division steers technological initiatives for Toronto's Municipal Licensing & Standards division, which handles the administration of the City's bylaw enforcement officers, as well as bylaw enforcement for Toronto Public Health and Toronto Fire Services. This suggests that *some* form of "law" enforcement falls under TSD's regulatory domain, but formal policing in Toronto remains beyond TSD's scope.

Even greater coverage gaps exist within the City of Toronto's procurement models, which appears as though it may apply to Toronto policing institutions but ultimately fails to do so. Procurement is the act of obtaining or purchasing goods or services, typically for business

purposes. In the public sector, procurement is bound by a process of competitive calls for proposals, intended on keeping the process open, fair, and transparent for all potential applicants (Bauhr et al., 2020; Vagstad, 1995). As I learned by attending a "Doing Business with the City" webinar hosted by the City of Toronto on April 5th, 2022, procurement in the City of Toronto is undertaken by the Purchasing and Materials Management Division (PMMD). At the highest level, the procurement process works as follows. First, City divisions determine what projects they need done, services they need rendered, or assets they need to acquire, and then report their needs to PMMD. PMMD then sources those requests, issuing solicitations on their procurement network (strangely called SAP Ariba). From here, bids are then received, evaluated, and rewarded, thus bringing the procurement cycle to a close.[14]

However, municipal procurement regulations *do not apply to municipal police* in Toronto, despite the suggestion that they would and should. In the procurement webinar I attended, I was told that the City of Toronto *does* oversee procurement for the TPS (see Figures 3 and 4). However, when I followed up with an individual from PMMD to confirm and ask questions about this association between PMMD and TPS, I was told that the slides are outdated. Even though the TPS are technically a public municipal service, the TPS' technology procurement regime is entirely separate from that of the City, once again allowing Toronto police institutions' use of technology to evade capture by municipal governance regimes.

[14] PMMD division oversees four types of requests: requests for quotations, requests for proposals, requests for tender, and requests for offers to purchase. Under a request for quotations, the lowest bidder meeting the City's requirements will get the contract. Requests for proposals (RFPs) are more exploratory requests, whereby the City gauges what solutions, methodologies, or products are available on the market and which of those align best with the general scope of work for which these proposals are being sought. Requests for tender primarily apply to construction or construction-related projects and are similar to requests for quotations; the City will have an engineer mock up an idea, and the lowest bidder meeting the project's specifications and requirements will get awarded the contract. Finally, there are requests for offers to purchase, which fall under the procurement banner but in reverse: in an effort to maximize whatever returns or residual values certain City-owned assets hold, the City will put up a request for offers to purchase these assets and sell the assets to the highest bidder.

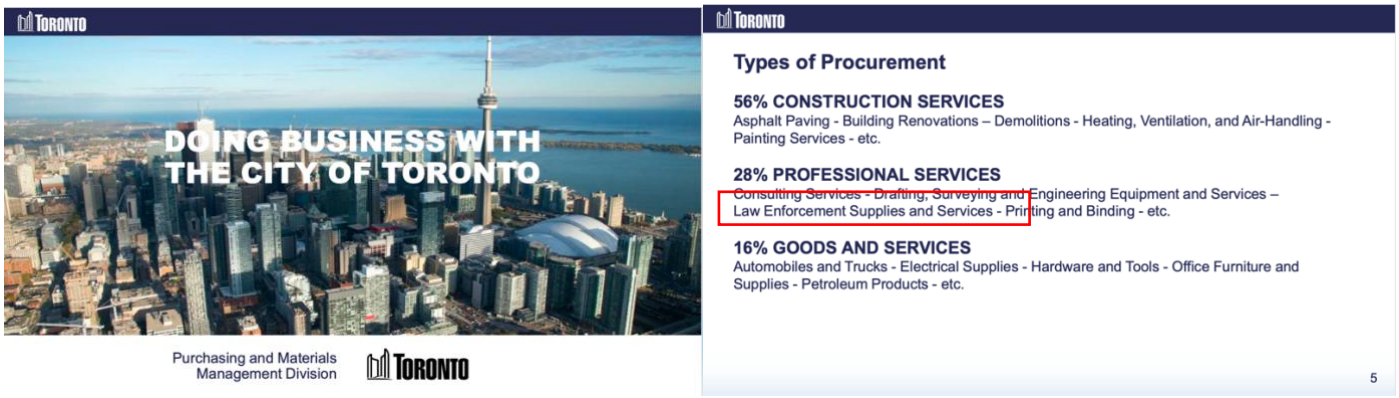

TORONTO
DOING BUSINESS WITH THE CITY OF TORONTO
Purchasing and Materials Management Division
TORONTO
TORONTO
Types of Procurement
56% CONSTRUCTION SERVICES
Asphalt Paving - Building Renovations – Demolitions - Heating, Ventilation, and Air-Handling - Painting Services - etc.
28% PROFESSIONAL SERVICES
Consulting Services - Drafting, Surveying and Engineering Equipment and Services – Law Enforcement Supplies and Services - Printing and Binding - etc.
16% GOODS AND SERVICES
Automobiles and Trucks - Electrical Supplies - Hardware and Tools - Office Furniture and Supplies - Petroleum Products - etc.
5

Figure 3: Slide deck from "Doing Business with the City of Toronto," showing reference to the City of Toronto overseeing procurement for the TPS (emphasis added)

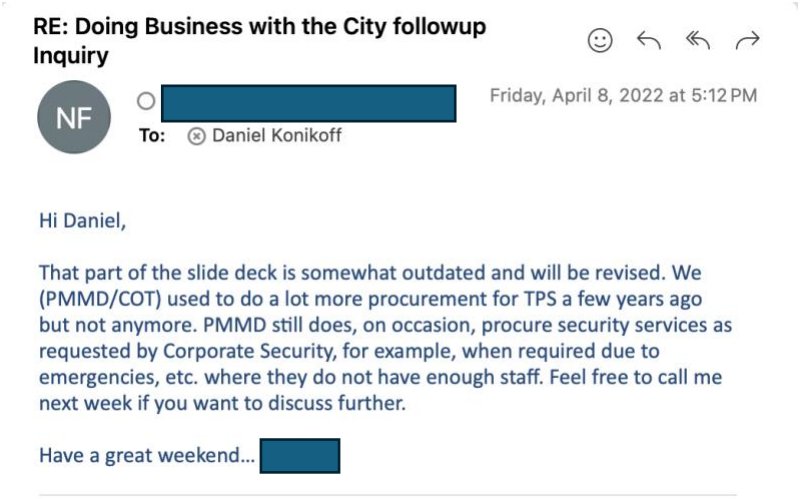

RE: Doing Business with the City followup Inquiry
NF
[redacted]
Friday, April 8, 2022 at 5:12 PM
To: Daniel Konikoff
Hi Daniel,
That part of the slide deck is somewhat outdated and will be revised. We (PMMD/COT) used to do a lot more procurement for TPS a few years ago but not anymore. PMMD still does, on occasion, procure security services as requested by Corporate Security, for example, when required due to emergencies, etc. where they do not have enough staff. Feel free to call me next week if you want to discuss further.
Have a great weekend... [redacted]

Figure 4: Email response from procurement specialist from City of Toronto regarding inquiry about any overlap between PMMD and TPS.

Similar regulatory vacuums exist at the provincial level, allowing provincial policing to evade governmental regulation of their use of technology. After speaking with a member of the TPSB involved with drafting the Board's AI Policy, I was directed to get in touch with Ontario Digital Service (ODS), a provincial ministry self-described as "a hub of technologists, designers and digital government experts who deliver user-centred products and digital policies using agile processes and data-driven methods" (ODS, "Overview," n.d.). Created in 2017, the ODS collaborates with other provincial ministries "to deliver services that make interacting with government simpler and easier for people and businesses" (ibid.). My TPSB contact suggested I

reach out to the ODS because the ODS "deal with AI in general" at the provincial level, and because my contact believed the ODS was working with the Ministry of the Solicitor General (SOLGEN)—the ministry responsible for oversight of the Ontario Provincial Police (OPP)—on better implementing AI into provincial law enforcement.

When I reached out to a policy expert at the ODS, I learned that my TPSB contact was half right: the ODS and SOLGEN had indeed been collaborating, but not on AI. Rather, the ODS, SOLGEN, and the private police technology company Axon Canada[15] had been collaborating on establishing a new a Digital Evidence Management program for the province. This digital program was implemented to facilitate data-sharing among police forces within the province (Solicitor General, January 19, 2021). Like my contact guessed, the ODS was indeed doing work on AI, but as it turned out, ODS' AI work did not apply to provincial policing. The ODS were developing what they referred to as a Trustworthy AI Framework, essentially a guidance document for steering the public institutions within the Government of Ontario use AI- and data-driven tools in ways that are transparent, explainable, fair, safe, and accountable (ODS, "Trustworthy AI Framework," May 6, 2021; ODS, "Principles for Ethical Use of AI," January 7, 2022).

I soon learned that there was ambiguity about whether this Framework would apply to provincial policing, and if it did, to what extent it would actually hold the OPP to any binding or enforceable regulations. In speaking with an individual from ODS who had helped develop the Trustworthy AI Framework, I learned that though the Framework would apply to provincial public services like SOLGEN, it was possible for the Framework to not apply to the OPP, despite the OPP's status as beneath SOLGEN's oversight. Nor, for that matter, would the Framework be binding; instead, the Framework would offer a collection of best practices meant to steer public service operators toward proper AI implementation without establishing enforceable regulations should a public service fail to meet the Framework's standards. ODS' position within the broader AI governance patchwork is thus a weird one. Overall, ODS can influence *some* policing practices in the province, as seen through their role in upstarting the Digital Evidence Management program for Ontario police departments. However, ODS are unable to either promulgate or enforce binding standards or to govern law enforcement's use of AI in the province. So while the Ontario Provincial

[15] Axon is best known as the company behind TASERs and body-worn cameras. However, Axon has continued to expand both its product and customer base. Scholars like Christopher J. Schneider and Erick Laming have recognized this expansion for what it is, identifying Axon as having a "looming monopoly" over digital technology in Canadian policing\ (*Hamilton Spectator*, January 31, 2021)

Police may fall under the banner of a public service, they are ultimately not under the purview of key public directives.

Similar coverage gaps exist at the federal level of Canadian government, as federal institutions that govern either policing or technology have struggled to regulate police technology. One example is the Directive on Automated Decision Making, established in 2019 by the Treasury Board Secretariat (TBS), a management committee that oversees the operations and administration of the federal government. The Directive was established to "guide the adoption of automated decision making at the federal level" and ensure that all federal institutions deploying AI do so in a way that is "efficient, accurate, consistent, and interpretable" (Scassa, 2021, p. 251). As part of the Directive, federal institutions producing or sourcing AI tools must complete what is referred to as an *algorithmic impact assessment* to evaluate the tool's potential for risk and harm to privacy and human rights (TBS, "The Directive," date modified April 25, 2023). However, the Directive is not enshrined in law, and the TBS lacks the authority to audit, investigate, enforce, or order federal institutions into following the Directive.

This poses problems for the governance of technology within the RCMP. The RCMP qualifies as a federal entity, and as such, falls under the authority of the TBS and its Directive. In conversation with an RCMP administrator, I was told that the RCMP *does* follow the Directive because they feel as though they have to. Internally, however, the specific legal requirement for the RCMP to follow the Directive when acquiring AI tools has not been clearly or explicitly defined, nor is it enforceable. Thus, because the Directive lacks "the force of law," it struggles with what the Privacy Commissioner of Canada identified as "limited compliance from the federal government institutions subject to it" (OPC, "Key Issues Related to Privacy," November 7, 2022). This "limited compliance" piece is key: it paints a picture of compliance as something better achieved by binding regulation and suggests that governance of how public institutions like the RCMP use AI is only as strong as the framework enforcing it.

What is more, the Treasury Board Secretariat's Directive on Automated Decision Making features a notable carveout that could exempt the RCMP from subjecting certain AI technologies to algorithmic impact assessments. Specifically, in outlining the scope of the Directive on Automated Decision Making, Section 5.1 of the Directive states that "This Directive applies only to systems that provide external services as defined in the *Policy on Service and Digital*" (TBS, "The Directive," date modified April 25, 2023). This Policy defines "external services" as "a

service where the intended recipient is a client that is external to the Government of Canada" (*Policy on Service,* date modified August 2, 2019). However, many of the AI systems the RCMP use in investigations provide *internal* services for government rather than external ones, with RCMP officers being these tools "intended recipients" (ibid.). This would once again allow the RCMP to skirt governance stopgaps meant to regulate technology at the federal level.

As described in Chapter 1, yet another federal institution, the Office of the Privacy Commissioner of Canada (OPC), encounters similar challenges in governing the RCMP's use of technology. However, additional tensions emerge at the intersection of the OPC, the Treasury Board Secretariat, and the RCMP's conflicting authority and mandates. As mentioned, the OPC has a number of responsibilities, but one of its main duties is overseeing federal institutions' compliance with Canada's *Privacy Act,* which governs the personal information-handling practices of federal government departments and agencies. But the OPC does not have to do this alone. The TBS has a Policy on Privacy Protection which, in effect, helps the OPC enforce the *Privacy Act*. The TBS' Policy on Privacy Protection includes a provision that requires all federal institutions to notify the OPC when a federal institution does anything that may impact the privacy of the people of Canada (TBS, "Policy on Privacy Protection," June 18, 2020). Under this Policy on Privacy Protection, virtually all government institutions, including the RCMP, must conduct what is referred to as a *privacy impact assessment* for new or redesigned programs, services, and technologies that raise privacy issues, and must loop the OPC in on the process.

However, in 2022, Privacy Commissioner of Canada Phillipe Dufresne pointed out a glaring contradiction emerging between the TBS' Policy on Privacy Protection and the OPC's oversight of the *Privacy Act*. Dufresne highlighted that although the Treasury Board Secretariat's Policy on Privacy Protection requires the RCMP and any government institution to prepare privacy impact assessments for the OPC's consideration, the *Privacy Act* does *not* have such a requirement codified in law, and that as a result, the RCMP often fails to submit privacy impact assessments to the OPC (Dufresne, "Appearance before ETHI Committee," August 8, 2022). The Privacy Commissioner used this example to show that there is *no legally binding obligation* for the RCMP to complete privacy impact assessments, and that the RCMP uses this tension to evade external regulation of their use of technology. Dufresne continued by pointing out a need for reforms to

address this gap—a reform which would have privacy impact assessments be included as a binding legal obligation in a modernized version of the *Privacy Act*.[16]

This example highlights the failure of soft law like best practices and policies to produce meaningful compliance, but it also highlights institutional frictions. Looking at the relationship here between the OPC, TBS, and RCMP highlights the complexity of governance networks, and how governance can actually fail when tensions between policies, laws, and institutions prove irreconcilable (Ansell & Gash, 2007; Bryson, Crosby & Stone, 2015; Duijn, Bannink & Ybema, 2021; Emerson et al., 2012; Thomson & Perry, 2006). When it comes to governing their use of AI and privacy-relevant technologies, the RCMP is positioned between two federal institutions—the OPC and the TBS—with two competing policies. And in deciding between them, the RCMP has—as the Privacy Commissioner seems to have suggested— preserved its own authority and oriented itself towards toward the institutions and regulatory artifacts with the least red tape.[17]

Consistent with this concern around what regulatory mechanisms carry with them the "force of law," the relationship between the RCMP and the Office of the Privacy Commissioner of Canada is further complicated by the OPC's "toothless" mandate. As I was told in every conversation I had with privacy professionals from across Canada, the OPC, along with all provincial and territorial privacy commissioners barring those in Alberta, BC, and Quebec, lacks what is referred to as *order-making power*. In other words, the OPC and certain privacy commissioners can only issue recommendations to institutions found to be in violation of privacy regulations, and these recommendations are neither binding nor enforceable. Take, for example,

[16] More information on this can be found in the OPC's 2022-2023 Annual Report to Parliament on the *Privacy Act* and the *Personal Information Protection and Electronic Documents Act* (https://www.priv.gc.ca/media/5996/annual-report-2022-23.pdf). The report states: "Our Office noted that, **despite requirements under the TBS Directive on Privacy Impact Assessment and the Policy on Privacy Protection, the RCMP had not submitted a PIA to us or notified us of the program.** During an appearance before the Standing Committee on Access to Information, Privacy and Ethics (ETHI), Commissioner Dufresne stressed that **these obligations – currently only policies – should be codified in the *Privacy Act* with clear and binding statutory provisions**. At the time of writing this report, **the RCMP indicated that it was working on a PIA, which we looked forward to reviewing**" (emphasis added, p. 11). Sassy!

[17] Yet another example of soft law failure and institutional friction can be seen in the Office of the Privacy Commissioner of Canada's Government Advisory Directorate, which "offers consultation services to federal institutions that develop programs and activities with privacy implications" (OPC, "Government Advisory Directorate," April 14, 2021). Institutions must reach out to the OPC for collaboration rather than the other way around, and there is nothing mandating anyone to take the OPC up on the Directorate's services. While the branch of the RCMP devoted to administering Access to Information requests has consulted with the Government Advisory Directorate, it is unclear if anyone from NTOP or the RCMP's technological units have capitalized on the Directorate's collaborative potential (RCMP, "Annual Report to Parliament 2021-2022," December 5, 2022; "Annual Report to Parliament 2022-2023," October 20, 2023).

the OPC's investigation into the RCMP's use of Clearview AI mentioned above, which culminated in the OPC's (co-)creation of FRT guidance and a recommended legal framework for law enforcement use of FRT.

An individual at the OPC who played a key role in drafting both the guidance and the joint letter explained the importance and necessity of these materials, but frequently expressed frustration with the limits of both the OPC's authority and the power of guidance. Guidance, this individual explained, is "an explanation of how to comply with the law," offering "the privacy commissioner's perspective on how one should interpret their privacy obligations with respect to [a] particular issue." OPC guidance, they added, serves an especially important purpose when technological innovation outpaces law:

> "So you'll have a thing like facial recognition technology that will come out, people will just start using it. The law is, like, 20 or 30 years old, that would be regulating it. So it doesn't say 'When you implement facial recognition technology software, you have to do X and Y and Z,' right? It just speaks broadly about privacy principles, and there's then a matter of interpreting how those principles would apply in any given specific scenario."

The FRT guidance, this individual added, emerged as a collaborative project between all provincial, territorial, and federal privacy commissioners, because "everybody has a stake" in the police use of FRT, and because "we figured FR is going to crop up in a police context across the board." This individual attributed the emergence of the guidance to the investigations into Clearview AI and the RCMP, but also recognized the uphill battle this guidance was facing. Specifically, this individual cited the ambiguous legal landscape in which police use FRT in Canada, as well as the OPC's abilities to "nudge" police rather than govern them outright:

> "So at the beginning of the guidance thing, so 2020, we were like, 'Okay, the police are using FR. So what's our response going to be?' basically. And what we figured was—we had the investigations—we figured we'll write a piece of guidance acknowledging that even though the existing legal framework for dealing with this stuff is probably not sufficient, the reality is that the police are going to use it. And we would prefer to be able to have some effect on nudging them towards using it in a more responsible way, rather than just charging ahead and doing whatever they want with it. So that was kind of the idea behind the guidance."

This OPC representative further elaborated on how the limitations of privacy guidance necessitated the OPC's creation of a recommended legal framework on police use of FRT. The purpose of the guidance, they reiterated, is not to make normative claims about what police's legal obligations

should be regarding FRT, but rather "to say, 'here's what you have to do to comply with the law as it stands today.'" However, this individual added that the OPC felt "very limited in what we can say" in this guidance, due in part to their claims that "the existing law is probably not really sufficient." This individual added that "if we [the OPC] want to say, 'The current law is deficient and we think it should be remedied by doing the following things,' that's got to be a separate document." The OPC thus promulgated its regulatory documents based on a view of what the law *should be* as much as an analysis of what it is.

The OPC, in effect, thus serves as a 'privacy watchdog' that works (much like the journalists discussed in Chapter 1) to identify problems *ex ante* and *ex post* so that publics and lawmakers are informed. But with this watchdog function, the OPC lacks the power to make binding rules and issue enforceable orders to institutions, and thus has little sway over how law enforcement in Canada *actually* use FRT (Government of Canada, "Challenges of the Current Model," August 16, 2022). The OPC reports to Canadian Parliament and can bend legislators' ears (or to quote the same OPC policy professional quoted above, "harp on the things we want" to the House of Commons) but according to this OPC policy expert, lawmakers "are free to ignore it." Thus, the FRT guidance and recommended legal framework emerge as documents of questionable regulatory utility—at least in terms of inducing and enforcing compliance with its view of the law. The OPC cannot issue institutions like the RCMP legally binding decrees that needs to be observed; it cannot force law enforcement agencies to comply with the advice its guidance outlines; and it cannot force legislators to change laws around FRT in policing. Instead, the most that the OPC and its FRT guidance can do is offer an informed perspective, meant to gently steer institutions toward compliance or reform without actually legislating or enforcing anything.

The individual with whom I spoke further expressed their frustration with this model by highlighting that the OPC does not necessarily want to be this way, and by pointing to what other regulators can do in other jurisdictions beyond Canada:

> "I mean, what we would *like* to be able to do—we don't have the powers to set rules in the way that others [might]. So if you look at the FTC [the US' Federal Trade Commission] or like, whoever, they have way broader powers. They can make orders, so they can say, 'You have to do this,' or 'You can't do that.' They can make rules in some cases where they'll say, 'Anyone dealing with X has to do Y,' they can do that type of stuff. We have none of that! So we're just...it's like a watchdog function, really. No rule-making power. This is a very contentious issue, by the way. It's very frustrating."

The OPC representative expressed similar frustrations with privacy commissioners' friction-filled challenges of regulating private enterprises, such as Clearview AI, and cited international governance models that were more appealing than the Canadian one:

> "We released a report of findings, and we said, '[Clearview is] engaging in these practices that we think are contrary to Canadian privacy law.' And [Clearview] were like, 'Well, we don't care.' And then what do you do? For us to pursue it, there's a mechanism for us to go to the federal court, but it gets really complicated and lawyerly. It's not a smooth kind of... Like in Europe, the privacy regulators can just fine companies. And they do that all the time, right? Here, it doesn't work like that."

This individual added, again echoing the capacity of journalists to shed light on controversial technological issues, that even though the OPC struggles to provide stable privacy governance via its watchdog function, that "you can get surprisingly far just on, like, public shaming, is sort of what it comes down to with certain institutions." But overall, this individual expressed friction inherent in the institutional structure of the privacy function in Canadian government, especially with respect to police technology: the OPC is not a regulator but nevertheless has regulatory ambitions. This, in part, might account for why the OPC collaborated with privacy offices from Alberta, British Columbia, and Quebec in their investigation of Clearview AI, as these provincial privacy offices *do* have the authority to issue binding orders to private enterprises.

One final tension worth highlighting within privacy commissioners' attempts at governing police use of FRT is the tension posed by federalism in both Canadian policing as well as the structure of Canada's privacy commissioner offices (Hueglin, 2021). Specifically, even though every privacy commissioners' office in Canada collaborated on the joint FRT guidance and the recommended legal framework, many of these offices do not actually have the authority to oversee the police use of FRT in their jurisdiction. This is especially apparent in the Territories, where territorial and municipal policing is carried out by the federal RCMP (RCMP, "Contract Policing," August 30, 2013).[18] And because the RCMP falls under the federal privacy commissioner's purview, representatives from every Territorial privacy office told me that their offices are powerless to govern police's use of FRT. Of course, there is power in showing all privacy commissioners united behind one issue, but this attempt at collaborative governance-making further highlights the limitations of certain privacy commissioners' authority in Canada.

[18] On top of all the Territories, 150 Canadian municipalities and every province except for Ontario, Quebec, and Newfoundland & Labrador have contracted out policing to the RCMP.

Overall, a number of Canadian bodies, institutions, and policies that appear able to govern aspects of policing or aspects of technology prove unable to govern police's use of technology, exposing a patchwork of actors and artifacts with hampered authority. Some institutions that are empowered to govern technology are not able to govern policing, their regulatory authority applicable only to narrow use cases or inapplicable to law enforcement. Similarly, institutions that have histories of working with policing in Canada or in other regulatory capacities find themselves unable to regulate the police's use of technology. Hierarchies of power, limitations in institutional structures, and absences of authority within these bodies and institutions external to policing ultimately lean in Canadian law enforcement's favour. The examples do not so much highlight police's raw power to ignore governance, but rather the lack of institutional authority of relevant governance bodies. This presents challenges for network and collaborative governance, and how the aims of certain governance bodies hinge upon police being willing and cooperative collaborators despite these governance bodies lacking the authority to make those collaboration happens. As scholars in these fields have shown, power imbalances are likely to exist in any form of collaboration, "since power is always unequally distributed across partners" in governance arrangements (Ran & Qi, 2019; cited by Wang & Ran, 2023). But while much of this literature has highlighted how actors in governance networks *overcome* power imbalances to ultimately achieve governance goals, I have demonstrated that in the world of police technology, a lack of authority on the part of institutions external to policing creates conditions for police technology to evade governance altogether (Hermansson, 2016; Purdy, 2012; Ran & Qi, 2019). This, I suggest, establishes a backdrop against which police are further empowered to build their own regulatory regimes as they see fit.

b. Regulatory Gaps within Policing

Police institutions' self-regulatory regimes similarly showcase profound coverage gaps that allow FRT and other technologies to evade oversight. These gaps predate the Clearview AI controversy, and many persist to this day. This highlights that though law enforcement's creation of internal policies, procedures, and programs are good starts, they struggle to make up for the omissions in the police technology governance backdrop that create permissive conditions for technological abuse. Much of this, I argue, stems from the *Ontario Police Services Act* (OPSA) and its 2019 update, the *Comprehensive Ontario Police Services Act*. These acts provide provincial and

municipal police the authority to self-regulate their use of technology without providing governance that is comprehensive or specific enough to capture police technology.

In Toronto, there are many sources of governance that oversee different aspects of policing, providing police with a framework for self-regulation. All governance to this effect is derived from the *Ontario Police Services Act* (OPSA)—provincial legislation overseeing all policing in the province.[19] The OPSA and its associated regulations establish five core areas of policing, including crime prevention, law enforcement, public order maintenance, emergency response, and victim assistance (TPS, RFP #1230424-17, n.d., p. 12). The TPS has derived ten other sources of governance from the OPSA and its regulations, including: "(1) Police services board policies and by-laws; (2) TPS Collective Agreements; (3) Standards of Conduct; (4) Service Governance Definitions; (5) Policy and Procedures Manual; (6) Routine orders; (7) Specialized manuals issued by the Chief of Police; (8) Unit-specific policies issued by the Unit Commanders; (9) Canadian Police Information Centre (CPIC) messages; and (10) Directions from a superior" (ibid.).

Between the OPSA and the ten sources of governance listed above, there exist many possible sources for the governance of police technology in Toronto, but I argue that many of these sources of governance fail to adequately cover police technology. I suggest that this problem begins at the top, with the OPSA's technological imprecision that provides little direction (and perhaps leaves too much room for abuse and misuse) to police departments on technological governance.[20]

The OPSA's technological imprecision is visible in both the dearth of provisions it actually *has* about technology, as well as the vagueness of the provisions that *do* address technology. For example, the OPSA recognizes the need for administration and infrastructure in support of policing's core functions. Under section 3 of the original OPSA, every municipality has to provide "adequate and effective police services in accordance with its needs, including all the infrastructure and administration necessary for providing these services, such as vehicles, boats, equipment,

[19] In 2019, the OPSA got an update with the *Comprehensive Ontario Police Services Act.* The Act includes the *Community Safety and Policing Act, 2019*, which is meant to replace the old OPSA. However, at time of writing, much of the new Act has yet to be fully enacted.

[20] For the sake of space, it is worth flagging that nearly identical concerns apply to the *Royal Canadian Mounted Police Act* (RSC, 1985, c. R-10). The *RCMP Act* gives the RCMP legal authority to operate as a federal police service in Canada, and contains provisions outlining the particulars of the RCMP's constitution and organization, the structure and duties of its external review committee, provisions about officer grievances and conduct (ibid.). However, the *Act*, does not contain any provisions pertaining to the force's acquisition, use, evaluation, and monitoring of technology. The dearth of centralized technological governance at the unit level within the RCMP was discussed in detail in the previous chapter.

communication devices, buildings, and supplies" (OPSA, 1990). The OPSA does not go into any more detail than that, allowing newfangled gadgetry to sneak into police departments within the wide umbrella that "communication devices," "equipment," and "supporting infrastructure" provides (ibid.). The OPSA thus provides an overbroad legislative requirement that establishes the bare minimum of technological governance.

The yet-to-be-fully-enacted 2019 update to the OPSA, the *Comprehensive Ontario Police Services Act,* is perhaps better equipped than its predecessor to handle cutting-edge digital technologies, but the only direction it provides on digital technology further places authority in policing institutions to develop their own policies without providing direction and what those policies should look like. Specifically, Section 39(1) of the updated OPSA empowers police service boards to "prepare and adopt a strategic plan for the provision of policing, which shall address," among other things, "(6) Information technology." The updated OPSA thus provides police with vague and imprecise authority related to technology. This further entrenches police's self-regulation of their use of technology without much oversight, providing minimal direction in how police in Ontario are to lawfully acquire and use technology in the first place.

The OPSA thus empowers Toronto police institutions to self-regulate via many of the other sources of governance outlined above, but institutional secrecy makes it hard to understand each of these governance sources' affordances and constraints. I was unable to learn more about how Toronto police institutions can govern technology through "specialized manuals issued by the Chief of Police," "unit-specific policies issued by the unit commanders," and "CPIC messages" as these are internal documents that I was unable to surface via FOI (TPS, RFP #1230424-17, n.d., p. 12). Same, by and large, with "directions from a superior," though the Routine Order issued by TPS Chief Mark Saunders to ban Clearview AI (see Figure 1 above) suggests that "directions from a superior" are perhaps more reactive modes of technological self-regulation than preventive ones (TPS, RFP #1230424-17, n.d., p. 12).

The sources of governance on which I *was* able to find information suggest similar coverage gaps regarding technology. For example, "Standards of Conduct" and "Service Governance Definitions" are outlined within the OPSA and enacted via Toronto Police Services Board policies. These standards of conduct and governance definitions, however, do not contain any specific directives on technology that particularly capture AI and FRT. Another publicly available source of governance, the TPS' Collective Agreement, provides a humorous example of

these coverage gaps. The TPS' Collective Agreement contains provisions about technology under Article 24, entitled "Technological Changes." This article stipulates that "Technological change shall be introduced after the Union and the Employer have consulted to protect employees from any adverse effect." However, the rest of Article 24 suggests that the Agreement's idea of technological change is somewhat narrow in scope, saying that "The Employer will ensure that, upon request from a bargaining unit employee it will retain the services of a qualified ergonomist to review their workstation to ensure that they are set up in an ergonomically appropriate manner" (TPS Collective Agreement, 2019-2023). To the Police Association and the Union, the governance of technological change is important, but less to do with reining in cutting-edge technology and more to do with occupational health and safety.

Further, an analysis of the 74 Toronto Police Services Board policies and 28 publicly available Toronto Police Service procedures[21] suggest that Toronto policing institutions were underequipped to handle the implementation of cutting-edge AI policing tools. Prior to and concurrently with the Clearview AI controversy, Toronto policing's policies and procedures only governed four distinct technologies and their uses: the police's use of body-worn cameras, the Service's closed-circuit television program, electronic monitoring of TPS employees, and in-car camera systems. I suggest, as do those within Toronto policing, that this lack of breadth in self-regulatory tech-governance infrastructure contributed the emergence of the Clearview AI controversy, but it also worth pointing out this infrastructure's lack of depth surrounding key issues like technological acquisition. Specifically, these policies and procedures take for granted and entirely omit the processes that brought those tools through the door in the first place; by the time procedures are in place, the technology appears to already be in use. Service procedures are an important part of the way the TPS governs technology, to be sure, but it is worth emphasizing how little is known about the way the TPS regulates technology's *acquisition*, which happens *before* procedures come into effect.

The procedures and policies that Toronto policing institutions created in the wake of the Clearview AI controversy—the ones the OPSA authorizes them to mount in the name of self-

[21] One civil society advocate who works on issues related to policing and technology told me that though a handful of TPS procedures are available to the public via the TPS' website, "you don't really get to see them necessarily. Because procedures particularly involving surveillance techniques and equipment…are considered protected by investigate privilege, and they're an internal matter, and it's more difficult to get in on any conversation of procedures, it's more difficult to get access to them." Still, the TPS' Procedures webpage is the closest thing the TPS has to publicly accessible regulations on technology.

regulation—have also shown coverage gaps that prevent comprehensive oversight of police technology. Though the TPS' AI Procedure is still in development, analysis of the draft version of the Procedure (which has since been removed from the TPS website) suggests a number of gaps, such as the lack of any requirements around the continuous monitoring, reviewing, and reporting on AI technology; a lack of detail around public consultation on AI technology; an insular AI evaluation committee comprised entirely of TPS personnel who alone possess the authority to decide when to consult external experts and communities. Thus, while the Procedure remains in draft form, AI remains underregulated and by and large ungoverned at the operational level of Toronto policing. What little we do know of this Procedure suggests that, despite the lessons of the Clearview AI controversy, coverage gaps on technology will persist in Toronto policing, further exacerbating police's capacity to self-regulate their technological toolkit.

Recent controversy has exposed coverage gaps in the TPSB's AI Policy, too. At a board meeting on January 11th, 2024, the TPSB presented its first update in almost two years since implementing its AI Policy and shared a preliminary inventory of technologies in use by the TPS. The TPSB identified five AI technologies in use by the Service, four of which the Board deemed to be of 'low risk' according to its risk assessment matrix: two automated license plate readers, an automated fingerprinting ID system, and a video evidence review software. The update shared that the TPS is also using one high-risk tool, a facial recognition system called NeoFace Reveal.

The update created controversy among civil society and governmental organizations. In a written response to the TPSB's update, the Ontario Human Rights Commission (OHRC) accused the TPSB of failing to meet the transparency and assessment criteria it set for itself. The OHRC says that though the TPSB assessed this tool as high risk, they failed to explain the reason for the risk level, outline a plan to pause the tool, evaluate potential risks, provide a comprehensive mitigation strategy, or even clarify whether it is seeking approval for continued use (DeGuire, 2024). The update raised alarm bells for the Information Privacy Commissioner of Ontario (IPC), too, who wrote a response to the update disagreeing with the way the AI Policy's framework evaluates risk. None of the four technologies labeled as "low risk," wrote the IPC, should be classified as such under the Board's own Policy, since the use of the four low-risk tools "could be used to assist in the identification of individuals for the purpose of their arrest, detention or questioning" and can even "link biometrics to personal information"—language explicitly contained in the AI Policy under "high-risk technologies."

Though the TPSB has not issued a response to these concerns, the conflict highlights coverage gaps in police self-regulation of technology, showing how the TPSB's capacity to administer its own risk assessments and set its own transparency criteria creates gaps through which technologies may evade governance and scrutiny. Further, this highlights the importance of an analytical lens that centres controversy, as it shows how reforms may emerge from crisis while being cause for tension and disagreement of their own (Bijker & Pinch, 1987; Epstein, 1996; Jasanoff, 2012; Nelkin, 1971; Nelkin, 1974; Venturini, 2010). While Chief Saunders' edict banning Clearview brought closure to the TPS' controversial *use* of the tool, the TPSB's attempt to further close the controversy of FRT governance via innovative reform has created *more* controversy, pointing to new and emerging conflicts between stakeholders. It has also shown the Policy's ineffectiveness in capturing a wide bevy of technology and TPSB's lackadaisical approach to following its own prescriptions. As a result, institutions with a stake in the governance of police technology, and who had already consulted on the development of the TPSB's AI Policy, have used these failures as an occasion to provide *more* critique of the Policy, in an attempt to steer the TPSB's AI governance in its intended direction. This once again highlights how governance networks form around controversy, while also highlighting how tensions can lie at the root of collaboration (and how collaboration may be something stakeholders force upon police in the event that police do not solicit that external feedback themselves) (Agranoff & McGuire, 2001; Bryson, Crosby & Stone, 2006; Frederickson et al., 2015; Rhodes, 1996; Wang & Ran, 2021). Thus, the TPSB's AI Policy emerged specifically from journalistic coverage of Clearview AI, and its roots lie in police use of FRT. However, I suggest that the recent concerns flagged by the OHRC and the IPC not only point to a policy ill-equipped at providing oversight to new FRT, but also ill-equipped at governing the use of *other* technologies, too.

c. Collaborations as Reinforcements of Police Power and Autonomy

The conflict outlined above provides a launch point for unpacking 'the stakeholder consultation' as a mode governance in and of itself, as well as process for making governance reforms. Emerging at the intersection of internal and external modes of police governance, stakeholder consultations can be collaborative governance practices that police mount to involve outside groups and individuals in policymaking. However, in the case of municipal and federal policing institutions, consultations can reveal tensions between actors and groups. Specifically, they can surface police's

most insular tendencies and leaving police in charge of dictating the consultation's shape, who gets consulted, and how much external feedback gets acknowledged. By exploring the TPSB and TPS' approach to stakeholder consultation, I argue that "consultative" modes of governance are often framed as collaborative and participatory modes but are by no means as collaborative as they seem, with police ultimately wielding power as a *veto player* to reject conflicting public feedback (Tsebelis, 2000; Ganghoff, 2003). I also look to the RCMP and NTOP to show how police's status as power-wielding veto player is also reflected in their decision to hold *internal* consultations, which cuts off the public and other stakeholders external to policing from processes of co-producing governance materials. Overall, I demonstrate that policing's approach to stakeholder consultation do not always align with the civilizing or participatory co-construction of policy (Chavis Simmons, 2007; Hill, O'Connor & Slane, 2022). Instead, the municipal and federal approaches to stakeholder consultation strain collaborative governance frameworks, showing how tensions between police and external actors hinder collective governance processes.

According to many participants with which I spoke throughout this project, stakeholder consultations in the world of policing come with a bit of a reputation: if they happen at all, they can be an unsatisfying box-ticking exercise that makes little impact. "One thing I struggled with is this perception, not completely unjustified given history," says an individual with a role in informing the development of the TPSB AI Policy, "that consultations are just a checkmark. And, you know, a lot of the people that we spoke with…assume that, you know, we're talking to them, and then we're going to ignore it and keep doing what we want." In mounting the public consultation on the TPSB's AI Policy, this individual told me that they actively wanted to counter this notion and create a structure of meaningful stakeholder engagement. And to be sure, some participants with whom I spoke thought this paid off. Among civil society groups, for example, some reported that they were impressed with the TPSB's willingness to collaborate. One such civil society advocate told me that on the TPSB AI Policy, the TPSB was willing to have "constructive conversations," listen to "full and frank feedback" on confidential drafts of the AI policy, and that this individual "could point to the lines [of the publicly shared AI Framework] where based on the conversations that I and other civil society actors had with them, the draft policy has been substantively changed."

Others, meanwhile, were less enthusiastic, pointing to police's abilities to shape consultations in their favour. After all, police services wield tremendous power in this equation.

In opening the policymaking process up to outside engagement, police still have the final say in whether to implement what has been suggested to them, acting as gatekeepers of (external) recommendations, only letting through the gates that which makes sense to them or that which is advantageous. And it is ultimately up to police to decide what these consultations look like—if they even deem them necessary.

The police's power to shape consultations can mean restricting external perspectives and keeping consultations exclusively in-house. This is what happened at the federal level with the RCMP and their development of NTOP. Internal documents reveal that the only group external to the RCMP that was consulted in the development of NTOP was the Office of the Privacy Commissioner of Canada. There is little information explaining what those consultations looked like beyond the occasional check-in with the OPC's compliance team. Nor, for that matter, was this collaboration done on the RCMP's own initiative. Instead, whatever collaboration occurred between the RCMP and OPC in the creation of NTOP appears to be because of the OPC's recommendations in light of their investigation into the RCMP's use of Clearview AI.

Barring potential collaboration between the RCMP and the OPC, emerging NTOP administrators at the RCMP did not conduct external consultation in the creation of their technology onboarding program. Instead, they embraced a consultative scheme that puts most governance-making power in the hands of police. Internal documents about NTOP reveal the extensive *internal* consultations the RCMP conducted, neglecting consultations with the public and other external stakeholders in favour of exclusive consultation with branches and units across the force, such as Legal Services, the Access to Information team, and more. Of course, internal consultation proved helpful for revealing, as mentioned in the previous chapter, the decentralization of technological governance in the RCMP. For example, my FOI of the RCMP unearthed a "Technology Owner Engagements Summary," which provides a summary of NTOP administrators' consultation with 10 different RCMP branches and units on their processes for evaluating and acquiring new technology (A0764529, pp. 395-397).[22] This information is valuable

[22] Of the 10 surveyed units, nine noted that they had no current policies or procedures in place for acquiring and evaluating technology. Most stated that they would conduct informal research and hold in-house discussions about tools and technologies before "escalating the request to procure" (A0764529, pp. 395-397). Some mentioned that they would occasionally involve the Legal department to assess the legality of certain tools, while others explicitly would *not* involve Legal. Some units stated that they would continuously review technology but that there was no formalized process for doing so and no generated documentation—while others highlighted that they did *not* track or monitor the tools' capabilities after the fact. Almost all units highlights that they would need assistance with conducting privacy impact assessments and navigating procurement processes, and that they did not have this assistance otherwise. Others

for ensuring NTOP meets agency needs, but it suggests that the rigour of RCMP's *internal* consultations allowed the RCMP to elide meaningful *outward* engagement. As a result, the RCMP deprived the public and civil society the power to shape and influence police technology governance at a national level.

Police can also shape consultations to be somewhat more outward facing than those in the RCMP example above, while still exercising power to narrow the consultation's scope. For example, when the TPSB began developing their AI Policy, they engaged in what several members of civil society referred to as a "pre-release consultation" or a "hidden public consultation phase,"[23] where key stakeholders from relevant organizations (academic institutions, civil advocacy group, professional associations) were identified and sent a confidential version of the policy for early feedback. The point, here, was—according to an individual involved in drafting the TPSB AI Policy—to subject a draft version of the Policy to expert scrutiny to "remove the big red flags" before the Policy went public. "If something is absolutely going to be abhorrent to the public," they continued, "we don't want that to be in the public draft, because then everybody will gravitate to that and we won't get a lot of helpful feedback. When you work directly with these organizations," they concluded, "you get that feedback a little bit more softly." This tows a line between transparency and secrecy—police are, in effect, choosing both *when* and *to whom* they are being transparent, sharing drafts with a narrow selection of stakeholders, but are doing so, perhaps, in hopes of yielding a more productive process of democratic engagement later on. Still, the TPSB's hidden consultation phase amounts to sanitizing policy before-the-fact, conducting a sample testing in secret so they can determine what is, in fact, "abhorrent," and dismissing the public's potential for providing "helpful" feedback.

The ability for the TPSB to focus group a confidential version of the AI policy before sharing a more refined version with the public reaffirms the control that policing institutions have over shaping the flow of stakeholder engagement, turning the consultative spout on and off when they see fit. That same representative from civil society who spoke to the TPSB's willingness to engage in "constructive conversations" still flagged a chronic concern with Canadian police writ

---

stated that decisions to acquire technology came down to "previous experience/knowledge & common sense" among unit members, and that units would "rely on the good faith of members to come to them when there is the desire to use a new tool" (ibid.).

[23] Funny enough, I actually was a part of these pre-consultations for the TPSB AI Policy, where I got to work on an early draft of the framework before it went out for public response.

large: that oftentimes, police are either looping in stakeholders for consultations "about technology [they've] already got a budget line item for," bringing in consultations far too late, or not looping external stakeholders in at all. In these situations where police bypassed external consultations completely, certain stakeholders like civil advocacy groups could elbow their way into regulatory debates, imposing their consultative perspectives onto a police institution who had otherwise ignored them. A representative from a civil society organization who played a role in advocating against the TPS' proposal to buy ShotSpotter told me that successful advocacy around ShotSpotter was a rare win: it was "one of the only examples…where we were able to intervene at the point before they paid out the money and were committed to using [the technology]." It was such a challenging endeavour, they added, because the advocacy group had to "insert [themselves] into those conversations" to which they had otherwise not been invited. This demonstrates the power imbalance between police and external stakeholders: the power police have to exclude groups from collaborative technology governance, and the uphill trek that external stakeholders like civil society advocates have to overcome to have their voices heard.

But being excluded from consultation processes, or participating in consultations but having feedback ignored, was something to which many stakeholders outside of policing were unfortunately resigned. One policy expert at a provincial privacy commissioner's office told me that privacy commissioner consultations with police is something that could happen "in theory," but only "if [police] wanted to reach out to [privacy offices] and ask for [their] thoughts," suggesting police forces. What is more, those who have the chance to provide feedback are similarly resigned to the chance that their feedback will be heard. A policy professional from a human rights organization in Ontario used similarly noncommittal language here in discussing their consultation to the TPSB AI Framework, saying that consultations are an opportunity for them to say, "We *think* you should take note of the following things," recognizing the upward limits of their power as an organization who can only provide recommendations but nothing committal. One individual from a police accountability advocacy group was far more blunt: the TPSB "always ignore[s] anything we've suggested," revisions to their AI Policy included. Consultations can thus appear cynical as stakeholders from advocacy, civil society, and government find themselves caught in a seemingly collaborative consultation while recognizing police's ability to "veto" external feedback (Tsebelis, 2011).

The TPSB's public consultation on the making of their AI Policy illustrates the unfulfilling potential of public consultation. At the end of 2021, the TPSB launched a public consultation to solicit feedback that would ultimately inform the final shape of their proposed AI Policy. The consultation appeared to be a gesture of goodwill: an effort to make up for keeping everyone in the dark about Clearview by proactively advertising that the Toronto Police is now committed to putting guardrails up around technology and taking public feedback seriously. However, the public consultation elicited a large amount of commentary that the TPSB flagged as being unable to implement into the final policy (TPSB, "Board Meeting Agenda," February 28, 2022). The TPSB explained that numerous commenters raised "more generalized concerns regarding the use of AI technology by the Service or police services generally," and expressed a belief that AI is "inherently extremely risky and should never be used" (ibid., p. 90). In other words, members of the public used the consultation process to query police's legitimacy, and whether police should adopt advanced technologies at all. These concerns, the TPSB said, were unable to be incorporated into the final AI policy; according to the TPSB, "AI technologies are ubiquitous in today's world," and the purpose of the proposed policy is about "permitting the use of AI technology…with appropriate safeguards" rather than prohibiting AI entirely (ibid., p. 90). The consultation, in effect, took the use of AI in policing as a foregone conclusion, a baseline premise, rather than interrogating the necessity of the technology in the first place.

Many civilian participants in the public consultation identified the consultation process as a police 'sales job,' accusing what might otherwise be considered a transparent and participatory mode of governance and policymaking as an opportunity for 'marketing.' One submission stated, "This [consultation] is a valuable effort for Toronto Police Services to helm a little PR." Another referred to it as transparency theatre, elaborating that:

> "I am a bit surprised to see how fast the turnaround is for this public consultation, considering the TPS is supposedly introducing this come February 2022. If you were to actually take the public's thoughts and concerns into account, you would allow more time to examine and respond to the inquiries. This feels to me as a **'box being checked'** just so the TPS can cover their tracks when the organization has every intention of going ahead with this technology, and in fact have already been using it."

Submissions highlighted a key issue otherwise not fully explored: Toronto Police had adopted risky, sophisticated technologies during a moment of marked public distrust in both policing *and* AI technology, and most especially at their intersection. One consultation stated, "The Toronto

Police have shown the communities in Toronto and beyond that they cannot be trusted. Offering more funding and resources at this point is unacceptable. Even minimal risk technology increases the risk of police causing further damage to society through their continued abuse of power." Another states, "I am not a technophobe…but when dabbling in such deep waters as AI, it is essential that utmost care be taken in how to navigate such technologies, and such care is something that the cops of this city have consistently failed to show, year after year."

Other submissions to the public consultations made gestures to more specific instances of untrustworthy policing in Toronto (such as the death of Regis Korchinski-Paquette), and other submissions referred to empirically supported claims about AI's propensity for racial discrimination and privacy violations, but many of these submissions highlighted the intersectional concern of AI's tendency to exacerbate policing's worst outcomes. Still, these valid concerns were by and large dismissed by the TPSB, who deemed these worries as something that could not be incorporated into the final policy—a policy whose goal is to allow for police to use AI. Thus, public consultation submissions framed the police's use of FRT and AI as enough of a risk to disqualify police's use of these technologies altogether. Police, on the other hand, vetoed these submissions, and framed technology not only as operationally necessary but as something they had already decided on using (Ganghof, 2003 Tsebelis, 2011; Vigour, 2014).

This demonstrates several things, namely the power police wield in public consultation processes: the power to pick and choose what suggestions they accept and which they reject. The TPSB's public consultation surfaced attitudes from members of the public that were critical of policing as an institution, critical of technology, and critical of the former's use of the latter, but many of the most fundamental and existential concerns expressed within the public consultation submissions were outright dismissed and deemed unimplementable. Here, the TPSB demonstrated its status as veto player, exercising its power not only to turn the consultation spouts on and off, but its power to undermine the otherwise democratic process of public engagement.[24] This demonstrates what scholars like Cheng (2024) flag as the "illusion of public input"—an illusion

[24] The same can be said about the TPS' public consultation for its AI Procedure. The TPS gave the public a one-month window over the holidays in which to complete their submissions, and only received six submissions by consultation's end. The lacklustre approach to consultation even merited an op-ed in the *Toronto Star* by three scholars worried about the consequences of "narrow consultations" and how these are "not the actions of a police force committed to public engagement" (Linder, Jones & McKelvey, *Toronto Star,* January 12, 2023).

bolstered by an unequal power dynamic that creates the impression of meaningful collaboration, but which allows police to pick and choose who they listen to and when.

Of course, independent scrutiny of police is a crucial component of democratic policing, with an active role to play in fostering police legitimacy (Bayley, 2006; Berkeley, 1969; Bonner, 2020; Jones et al., 1996; Manning, 2016; Prenzler & den Heyer, 2015; Stone & Ward, 2000; cited in Kwon, 2022). This, on paper, is what police-led consultations—with the public, with civil society actors, with government bodies—appear to be: an act of democratic accountability gathering knowledgeable stakeholders and interest groups into the fray for participatory governance. And this is what having some sort of sturdy legislative backdrop—one devised by a government external to policing—appears positioned to provide. But given patchy legislative structure with coverage gaps, as well as performative stakeholder collaboration, police are given even more power and authority to govern their own use of technology. Of course, it is not news that 'police end up on top' in yet another context. It is, however, worth highlighting, since the stated goals of most of these governance initiatives proposed in Clearview's wake were to give the public a greater voice in a process that famously caused controversy for neglecting public stakeholders.

External stakeholder collaboration around police technology governance can thus bear the appearance of a collaborative governance effort, all while failing to deliver on that to which collaborative governance aspires. When they happen, these external consultations appear built on reciprocity and the sharing of power, with police inviting disparate stakeholders to engage in collective decision-making around a controversial subject (Ansell & Gash, 2008; Emerson, Nabatchi & Balogh, 2012; Fadda & Rotondo, 2020; Fischer, 2012; Isett et al., 2011; Provan & Kenis, 2008; Wang & Ran, 2021). But these consultations are undone by shoddy execution that excludes key perspectives, stakeholder distrust, and police's authority to hold tight to decision-making power instead of sharing it (ibid.). This can be seen in the TPSB stakeholder consultations, which highlight the lack of trust the public has in police and in technology, civil society's concern around whether or not their expertise holds sway, and police's capacity to veto and disregard external stakeholder perspectives.

This chapter's focus on regulatory patchworks bears implications for controversy as a useful analytical frame in the study of police technology's governance. As shown by the TPSB's AI Policy's contentious public consultation, as well as the Policy's inadequate regulatory coverage

recently highlighted by civil society stakeholders, governance mechanisms designed to close controversies can simply fail to close them—and create *more* of them. By exerting strong unilateral control over the public consultation, Toronto police leave the lingering distrust from their secretive use of Clearview AI unresolved. And though the TPSB's AI Policy has been in effect for two years, the policy has recently bred *new* conflict, as stakeholders external to police have expressed their disagreement with how the policy works in action. Stakeholder conflicts old and new may thus arise within the processes of both developing and executing on governance.

But the TPSB and RCMP's strong unilateral control outlined in this chapter also point to a key problem not only emerging within the world of police technology, but one emerging in the world of AI more generally: that of self-regulation. Currently, debates are unfolding around the world about how AI should be governed, with some looking to governments and formalized regulation as the last bulwark between humanity and our robot overlords-to-be, and others pointing to the tech industry as capable of regulating themselves (Ferretti, 2022; Gabriel, 2020). Those in favour of the latter ask, "What do politicians know about technology?" and believe that the AI industry, and the AI industry alone, should set realistic-yet-high standards for aligning AI with human values and minimizing its potential harms (Hoffman, 2022). Meanwhile, those in the former camp see AI technologies as too consequential for their regulation to be captured by private interests, who could hold the power to veto regulations they deem financially inconvenient (Accountable Tech et al., "Zero Trust AI Governance," August 10, 2023). These same questions, I suggest, apply as much to AI in policing as they do to AI in general. As academic experts, industry leaders, and digital policymakers think through who should govern AI writ large, they will have to think through who will govern AI in policing—questions made all the more complex given the regulatory patchwork against which they are situated.

Conclusion

The thing about patchworks is that it is easy to slip between the holes in the fabric. Such is the case in Canada with police technology. Police technologies often evade governance because of institutional coverage gaps within the patchwork of bodies and institutions supposedly governing police technology. Some bodies, like Toronto City Council, govern aspects of policing but not police's use of technology. Other institutions, like the Ontario Digital Service, govern AI in the

province but not in policing. Still others, like the federal privacy commissioner, can intervene at policing and technology's intersection, but find themselves limited in regulating either.

Amidst these institutions of limited regulatory jurisdiction, police in Canada find themselves increasingly empowered to regulate themselves. This means police are free to develop their own technology policies and procedures without clear legislative direction or oversight on how to do so. It also means police launch uneven stakeholder consultations, reinforcing police's authority as unilateral decision-makers by virtue of how selective they are in terms of who gets listened to. It is easy to point to the many bodies, institutions, and actors with a stake in police technology—the city councillors, the privacy watchdogs, the civil society advocates, the plugged-in public, the tech-focused wings of various levels of government, the police themselves—and assume a network of interlocking actors smoothly steering police technology straight. It is easy to see all these actors *talking* to one another—police boards seeking civil society expertise; police administrators consulting with departmental units; citizens submitting comments on draft policies—and assume that this collaboration is premised on sharing power and reaching consensus (Ansell & Gash, 2008; Emerson, Nabatchi & Balogh, 2012; Fadda & Rotondo, 2020; Fischer, 2012; Isett et al., 2011; Provan & Kenis, 2008; Wang & Ran, 2021). But between institutional coverage gaps and selective stakeholder collaboration, a picture of police technology governance emerges: one in which police are the first and last arbiters of how their technologies are governed.

The following chapter reframes police's increasing regulatory authority over their own technologies through the politics of knowledge. Chapter 3 explores the secrecy that enshrouds policing and its implications for governance, showing how police assert themselves as holding unique expertise about police technology. This claim to expertise, as well as legal structures of ignorance-making, exacerbate distrust in police and undermine the governance of police technology in the process.

Chapter 3: Blue Walls, Black Boxes, and the Politics of Knowledge in Police Technology

Following the award ceremony is "How an AI Machine Trust Problem Combats Doubt in Modern Crime Fighting Tools," a panel featuring an all-Canadian lineup of representatives from the RCMP, TPS, and NuEnergy.ai, an Ottawa-based AI management software firm. The panelists wax poetic about waning public trust in both policing *and* AI technology, using this as a backdrop to unpack how their agencies have placed greater emphasis on following transparency the Clearview AI controversy. The National Technology Onboarding Program, says an RCMP representative, is about winning back public trust through technological accountability and "responsible" use of modern tools: if the people of Canada are to trust police, they "need to be *aware* of what technologies we're using." Later, in the Q&A, a spectator wonders how the RCMP expects to balance NTOP's lofty transparency goals with "criminals gaming the system." One of the RCMP representatives responds that the two are not mutually exclusive—the RCMP can "open up the transparency door quite a bit without giving up trade secrets"—but emphasizes that the risks are not worth the secrecy. "We shied away before," says the RCMP representative, but it pays to "explain the story" rather than "not telling them anything." To this, the TPS representative chimes in with a more cynical take on techy transparency. "What we're doing and what the public thinks we're doing," they say, "are miles apart." Transparently explaining technology is not so much an end to be pursued in and of itself, they add, but rather a technique that police departments like the TPS can use to "calm the conversation down" around police technology. Transparency, as well as "the ability to say 'oops,'" are the best ways to avoid what the representative from the TPS refers to as a "front-page police-pulling-the-wool-over-the-public's-eyes story."

Both the RCMP and TPS' views of secrecy, transparency, and trust showcase a politics of knowledge at play in the arena of police technology. To police, information about operational capacity is a precious commodity worth keeping secret, and police have structures and justifications in place to rationalize keeping their gadgets in the shadows. The Clearview AI controversy showed that this technological secrecy can have its downsides, compromising public trust in police institutions. But as I heard in the panel, technological transparency is at once a noble and instrumental practice. To the representative from the RCMP, technological transparency is an end in and of itself, something to pursue for the betterment of accountable police practices. To the representative from the TPS, transparency on police technology is an exercise in public relations, a means of quieting the storms of controversy.

In this chapter, I show how secrecy and ignorance about police technology are constructed (Barton & Davis, 2018; Bloch-Wehba, 2021; Ericson, 1989; Koningisor, 2023; Manes, 2019; Proctor & Schiebinger, 2008; Tombs & Whyte, 2003). I argue that knowledge about police technology is mapped onto an unequal power dynamic in which police maintain the primacy of their knowledge on technology while withholding that knowledge from stakeholders whom they dismiss as ignorant of how these technologies really work. Further, I build upon scholarship about how secrecy is endemic to all facets of policing and argue that police, private technology companies, and governmental institutions deliberately build technological opacity into laws, policies, and procedures (Chin & Wells, 1997; Conway & Westmarland, 2020; Conway & Westmarland, 2021; Koepke, 1999; Liu, 2020; Powers Jr., 2000; Westley, 1956). This constructs an architecture of secrecy around police technology, inhibiting external stakeholders from understanding police's digital toolkit or knowing what it contains. I contend that police institutions' efforts to control—and in some cases keep secret—knowledge about new technologies has implications for trust in and legitimacy of police, and compromises governance reforms that prioritize collaboration and transparency.

Constructing Ignorance, Marketing Transparency

My police informants often characterized controversy over police technologies *as a problem of knowledge*—and more specifically as a problem of public ignorance about these technologies and their uses. When it comes to knowledge and understanding of police technology, police perceive their own professional knowledge and expertise as superior, while constructing lay publics and those outside policing as "ignorant" and in need of careful "education" (Abbott, 1988). Throughout my research, I was told time and again by police professionals that most other stakeholders in Canada simply "didn't get it." A common refrain was that the police had a superior understanding of police technology drawn from their hands-on experience with the technology, as well as the information they received from private technology vendors, who would provide product data and company personnel to walk police through the ins and outs of technologies prior to making a sale.

Police use claims to professional expertise to argue that they should retain jurisdiction not only over police *uses* of FRT, but also over *knowledge about those uses*. According to police, it is everyone else—the public, civil society, journalists, and government—that are under false assumptions. One of these false assumptions, said police, is the widespread belief that Canadian

police were using facial recognition 'live': that these systems are linked to real-time surveillance tools, like body-worn cameras or CCTV. This was something that police—whether in interviews, in observation, or in internal documents—rejected outright: this might be true in other parts of the world, like the UK, they would say, but not here in Canada.[25]

Police would often rearrange their framing of FRT to frame facial recognition as technologically imperfect but beneficial and necessary to police operations. Police would express frustration that other stakeholders did not know that this tool, often maligned for the threats it poses to privacy, can actually be *good* for privacy. Facial recognition systems, some told me, can actually 'blot out' irrelevant faces in an image, protecting the privacy of other people who just so happen to be captured in a wider photo of a suspect. Police also maintained that those outside policing did not know that facial recognition is the most helpful tool for solving child exploitation cases and was a necessary tool on that utility alone.

To the police officials with whom I interacted, government and civil society stakeholders painted with too broad a brush, outright dismissing the positive role AI and FRT can play in policing in favor of a blanket rejection of these tools as concerning at best and destructive at worst. One panelist at an IACP panel about AI-enabled surveillance technology spoke of this standoffish relationship between police and external stakeholders, describing the ordeal and "public outcry" their police department had to get through to use a tool they wanted. "We were taking it pretty hard on the chin from the ACLU," said this presenter, referring to the American Civil Liberties Union. Not only did this individual say that their agency had to "battle the civil liberty groups," but they also had to build trust with a fundamentally wary and skeptical community—otherwise, the presenter added, "they'll think we're spying on them." Here, this individual was suggesting that standoffish stakeholders external to policing had the wrong idea about technology and its uses. But as mentioned, police institutions frequently do not disclose the tools in their technological toolkit or their methods of use. How could public stakeholders *not* be ignorant or skeptical under such circumstances?

The most common justification for actively keeping technology secret from the public and civil society was a common one: that disclosure would compromise the operational and tactical

[25] UK Parliament has launched an investigation into live use of FRT in an effort to render its use more accountable and transparent (UK Parliament, "Committee launches an investigation into Live Facial Recognition," December 11, 2023).

advantages conferred by the technologies.[26] In other words, they argue that going wide with what technologies they use and how they are using them would allow criminals to devise clever workarounds, something which Manes (2019) refers to as the "anti-circumvention" argument for police secrecy around technology (and something that the individual in the Canadian panel's Q&A championed as a necessity in police's knowledge management around technology).

To stakeholders outside of policing, the lack of transparency around technology was a mechanism police used to evade governance, but more importantly, it was conceived as another way for police to assert the primacy of their own knowledge about investigative practices. A member of a technology advocacy group, for example, told me that they were skeptical of anti-circumvention arguments. Police keep technology secret, they told me, "because they know [that transparency will] invite a lot of scrutiny and regulatory oversight that they don't want." A Canadian journalist who reports on police technology similarly dispelled the anti-circumvention justification, attributing police opacity on technology to what they believed to be an explicitly anti-transparent mindset. "[Police]," they said, "don't agree with or understand the idea that they should be transparent…And what we have now is a very paternalistic system where the police are saying, 'Oh, you're better off not knowing about [Clearview AI], we're gonna protect you from this information.'"

Surprisingly, some stakeholders *within* policing were critical of the abovementioned anti-circumvention argument popular within police circles. These stakeholders suggested that the primacy that police assert over their own technological knowledge is outmoded, impractical, and most of all unsupported. Ryan Prox, a veteran of the Vancouver Police Department who has spearheaded a number of technological initiatives like the VPD's use of GeoDash (and who insisted I use his real name rather than anonymize him), outlined that the anti-circumvention argument is based on instinct rather than fact, and that other police actually find it hard to describe *how* they expect criminals to circumvent police technologies at all. Discussing the acquisition and implementation of a GPS-crime mapping system in Vancouver, Prox told me:

> "There was a worry that now that we're announcing where the crime is happening, the criminals are now going to use GeoDash to circumvent our enforcement activities. So if we put that out there, it's going to be used against us. That was one of the

[26] In explaining the importance of transparency as a cornerstone of good governance of police technology, a member of a professional police association said to me, "So you've got to be able to be somewhat transparent in a way that still allows you to function." This phrasing implies that at a certain point, transparency requirements become a hindrance to police operations, with governance perhaps getting in the way of policing.

> justifications for not letting me launch this. And what I had to do is set up a questionnaire with the police department and said, 'Okay, we're gonna run it on a trial basis for four months, if we get any indication that the criminals are using this to co-opt us, we'll roll it back to a week. But I need reports.' So we put out surveys and said, 'Have you had any indication when you arrested a B&E that they're using their iPhone or whatever to look at where the crime incidents are taking place and then going somewhere else so to avoid an enforcement activity that may be taking place there. We had nothing. It didn't happen. It was just one of these 'sky is falling' Chicken Little things."

A representative from the RCMP's National Technology Onboarding Program echoed Prox's statement, saying that police can rarely articulate *why* technological capabilities should be kept secret. Regarding the notion that technological transparency would compromise the tool's effectiveness, I was told that oftentimes when officers bring tools to NTOP for evaluation, "they have concerns that if you disclose this information publicly, then we're never gonna be able to use this tool again." This individual empathized with those officers but explained that their concerns should not outright vitiate transparency. Rather, those officers should "tell us that and explain to us why, and let's develop a strategy for disclosing *as much information as we can* without compromising [the technology]." But even at that, this NTOP representative is skeptical of "the idea of [transparency] compromising the [technology's] effectiveness." "Everybody is hypersensitive," they tell me. "When you ask them, like, 'can you give me an example of how this will compromise,' it's like, there's never any real clear answer."

This representative also believes that the anti-circumvention argument is based in police's overestimation of criminal savviness, suggesting either a culturally ingrained kneejerk instinct toward secrecy, or a rhetorical argument to justify police keeping exclusive control of technological knowledge. "There's this expectation that criminals are out there scouring the internet looking for all the information on the tools that we use. The reality is that most criminals are not very sophisticated…the majority of crimes that the RCMP investigates will involve people who are not technologically sophisticated." It thus falls to governance regimes like NTOP to break through these anti-circumvention arguments for keeping police technology secret, but perhaps these justifications for technology's continued secrecy are far too stitched into the fabric of police culture.

To that point, most other participants from the world of policing with whom I spoke framed technological secrecy as a consequence of a police culture that stems from what many participants

bluntly described as poor "marketing" of technological knowledge. The implication of this language was that selective disclosure could be used to "sell" police vantage points without disclosing the nuts and bolts of methods and use. One member of the RCMP told me plainly: "Police officers are not very good at *selling* what they do. It's not in our nature to just sell what we do; we do policing, right?" When I asked a recently retired TPS officer of 35 years whether the police do anything to make people understand how technology works, they told me, "No. And that really is the short answer: we're doing a piss-poor job at marketing." A former officer with the TPS who has since moved onto a supervisory role at an overseas police department very much agrees: "And, you know, putting that kind of time and thought and energy into how you communicate, what you communicate, I think is big. Police agencies do not do this well. It doesn't matter where you are in the world." However, seeing as most modern police departments have well-developed media, communications, and public relations teams, the claim that police are bad at selling what they do feels only partially correct. A cursory glance at the websites for Toronto Police Service, Ontario Provincial Police, and the RCMP show "Feature Stories" of police doing "Movember" (Fanfair, *TPS,* November 1, 2023) how officers are bridging language gaps with Inuit communities (Poland, *RCMP Gazette,* October 12, 2022), highlights from the police dog championships (*OPP News,* September 25, 2023) or how a drunk driving stop actually led to police taking guns off the street (*OPP News,* October 13, 2023). The police, if anything, seem good and able to sell what they do, so long as they are selling that which has immediate relevance to their perceived public mission.

One police administrator told me that it does not matter if police do everything right on acquiring and evaluating technology on the back-end if it is not presented clearly and "sold" well to those outside of policing: "The worst mistake we've ever made with technology," they said, "is to do things in what I'll call kind of 'under the covers' of what we haven't *advertised*, you know, unawareness. And get caught later doing something that might have been acceptable and reasonable had it just been *marketed* properly" (emphasis added). An individual involved with creating the Connected RCMP's Digital Policing Strategy, a program dedicated to ensuring the RCMP has up-to-date technologies and equipment, similarly described the initiative as a "marketing scheme" designed to inform RCMP officers and the public about forthcoming technological solutions. A police administrator with which I spoke perhaps took this whole marketing metaphor to its extreme: suggesting how transparency might connect with public trust

in police, this police administrator referred to communicating openly about police use of technology as "making deposits in the bank of community buy-in."

Other participants from policing expressed their belief that sharing information about technology should not be done for its instrumental value, but for the sake of transparency as a public good. Vancouver police officer and secrecy-skeptic Ryan Prox, who claims that police's control over technological knowledge and the primacy police ascribe to operational secrecy is a fixture of policing that needs re-evaluating. "The other problem is, it's cultural," he tells me. "Yeah I'm a police officer, but I don't think like one…If I'm in meetings [about the use of technology], I'm like, 'Why don't we just put it out to the media?' And then people would be like, 'Whoa, what do you mean?'" To that, Prox believes that police's cultural inability to proactively "sell" their use of technology is out of touch with today's information ecosystem, and engaging in active transparency around technology will help police in the long run. "'What's the worst that can happen [from disclosing technology]? It's gonna come out at some point, we're gonna get hit with FOIs, they're gonna get it, we can't hold it, do it now. Get up front, get ahead of it.' It's rather that you're not in a defensive position, you're at least announcing, you're being transparent, you're trying to do the right thing."

To sum up, police often view public pushback against new technologies as a problem of knowledge and more specifically a problem of public ignorance rooted in misunderstanding of police professional knowledge—but they do little to meaningfully share knowledge about how they are using technologies with reputational issues. In fact, for many insiders, control over knowledge about the existence and uses of technologies is an essential facet of professional jurisdiction over policing (Abbott, 1988). Part of the argument for careful police control and curation of knowledge about policing technology rests on police understandings of secrecy as an essential part of policing techniques. Technology is, by and large, something to keep secret because of the (contested) operational advantages that secrecy (supposedly) bestows on police. Here, police rationalize their exclusive claims to authority over technological knowledge, not only because they know how these tools 'really work,' but because letting this knowledge out would compromise their occupation and the premium their occupation places upon such knowledge (Kroezen et al., 2013; Mclaughlin & Webster, 1998). And to the extent that police officials recognize the need to make the technologies more transparent, they often think of this as an advocacy exercise rather than a disclosure exercise, reducing transparency to a commodity rather than a democratic end in

and of itself. Police secrecy about their use of technology has proven, time and again, to be more trouble than it is rightfully worth. It was this lack of transparency that brought with it a firestorm of controversy about police technology, and about the obfuscated practices that get technologies like these into departments in the first place.

The Architecture of Secrecy

In addition to police's expert claims to knowledge, widespread ignorance of police technology is deliberately constructed by laws, policies, and organizational arrangements that keep the public in the dark about what tools police use and how those tools work (Barton & Davis, 2018; Proctor & Schiebinger, 2008; Tombs & Whyte, 2003). These laws and policies are the building blocks that make up an architecture of secrecy—a structural support for manufacturing ignorance on police technology in Canada. Some of these include structural limitations in how technological governance regimes are designed, as well as a lack of human and financial resources to support them. I will also highlight more concerning frameworks that construct technological ignorance, such as corporate limitations on proprietary knowledge, procurement frameworks that allow free trial technology to bypass transparency requirements, and FOI regimes that let police institutions keep technology out of public scrutiny.

One relatively banal component of policing's architecture of secrecy is the way in which governance structures and frameworks are actually designed. For example, in the speaking notes of a slide deck disclosed by the RCMP via FOI, a fundamental tension is flagged in terms of how NTOP's structure: its status as an approval body or an advisory body. To quote the speaking notes: "We considered whether NTOP would be an approval body (would strengthen accountability for technologies but could results [*sic*] in less flexibility and reduced buy in from programs), or an advisory body (lacks the ability to enforce decisions, risking irrelevancy if programs do not see value." (A0764529, p. 143). Because of "resourcing, existing approval structures and organizational realities," NTOP has accepted its role as an *advisory* body (ibid.). This creates a problem at the intersection of transparency and collaboration, also flagged within the speaker notes: "NTOP will only be as good as the information we receive from Divisions" (ibid.). Thus, the existence of NTOP does not automatically ensure the RCMP will be transparent about technology, as NTOP requires active collaboration with Divisions within the RCMP, some of whom may not wish to initiate the NTOP assessment process.

Further, participants often described the biggest structural barrier to sought-after technological transparency as a resourcing problem. These are issues that appeared in discussions with members with knowledge of the RCMP's development of NTOP and Toronto policing institutions development of the AI Policy and Procedure. In a draft risk assessment document surfaced via FOI, the RCMP stated that, "Without external pressure…there is a possibility that the resources required to implement and institutionalize the program will not materialize" (A0764529, p. 48). The RCMP forecasted that in order for NTOP to provide effective and transparent oversight of police technology, the program would need to hire 15 new employees—a process which would take between one to two years to fill (ibid.). What is more, NTOP would need a fixed $3-million annual budget to sustain its employees and their continued work assessing technologies and sharing information about them. Here, simple barriers to resources and structural concerns within the RCMP would be a concrete barrier to NTOP achieving technological transparency.

But as mentioned earlier, actors external to policing institutions can be important vectors of change. I was personally involved in breaking the story of NTOP's resource challenges with a reporter from Canada's national newspaper, *The Globe and Mail* (Freeze, 2022). After the article was published, a representative from NTOP told me that this article was instrumental in helping NTOP secure the funding it needed to operate and fulfill its transparency goals. This once again highlights the roles of journalists and researchers in the broader collaborative network around the governance of police technology, showing how actors external to policing can bolster reform efforts. It also underlines how essential resourcing and staffing are in technological transparency, and how understaffing and under-resourcing hinder what can be known about police technology.

I was told something similar by a representative from the TPSB, who mentioned that in developing the TPSB's AI Policy, resource constraints prevented police from meeting the demands of external stakeholders regarding technological transparency. Limits on resourcing, I was told, affected "what's feasible" in terms of how much information the TPSB could come to disclose about technology. This individual from the TPSB specifically pointed to a common refrain that arose during the public consultation behind the TPSB's AI Policy: the public desire for a greater frequency of public reviews and reports of TPS technology. However, this individual maintained that on a practical level, the frequency of transparency reports that external stakeholders demanded was not realistic: "doing a review of the technology every three months, is not going to be effective," they said, adding, "it's just going to be overwhelming." They added, "Those are the

facts: it's just impossible for the Board to become a body that deals with tech reports every two or three months. And not that we're planning on adopting that many technologies, but just thinking about the feasibility of it…" Again, structural issues of resourcing can interfere with transparency efforts like proactive reporting of technologies to the public: "How much reporting is just going to overwhelm the board? How frequent do reviews need to be made, taking into consideration the fact of their funding is not limitless and staffing is not limitless? So, for example, I know that a lot of the comments that we got is 'You should review these technologies every three months.' Yeah, that's a great idea. I'm not saying it wouldn't be good if we could. But the fact is, that's not our business." Relatedly, when I asked a representative from the TPS when to expect their AI Procedure to be formalized, I was told "I don't know—it's just me working on it." Resourcing thus becomes a structural issue that gets built into the architecture of secrecy around police technology. These issues are not necessarily malicious, but they do bear consequences for how much can ultimately be known about police technology. They also suggest an institutional decision to under-resource important governance measures.

One of the more insidious building blocks of this architecture of secrecy is the non-disclosure agreement (NDA). Most new digital and AI-driven tools, like Clearview AI's facial recognition system, are proprietary corporate products. Companies which sell these technologies to police often make police sign strict NDAs, preventing police from revealing their purchase or use of technology to the public (Manes, 2019; Siems, Strandburg & Vincent, 2022; Stardust, Gillett & Albury, 2023). To quote Elizabeth E. Joh (2017), what begins as an act "out of [a company's] private self-interest" has "considerable public impact" by undermining accountability and transparency of police technology (p. 19). In all likelihood, police using Clearview AI in Canada had to sign an NDA to use the tool Though there is no data confirming or denying whether Canadian policing using Clearview AI signed NDAs, an FOI disclosure to Legal Aid NYC shows email exchanges between an NYPD sergeant and a Clearview representative suggesting that the sergeant signed an NDA for use of facial recognition tool (Legal Aid NYC, n.d.). Overall, trade secrecy and the NDAs of which this secrecy is comprised serve as a bulwark to public scrutiny of police technologies, one which restricts police from disclosing technology's usage and, in so doing, cordoning off knowledge about technology as belonging to police and vendors alone.

Equally as important, private companies do not disclose their products' back-end code to police, instead selling them a pack-and-play policing product. In the language of technology

studies, police are simply another 'class of users' of, in this case, highly sophisticated computing technology. Most police officials will not have the same kind of knowledge about how the technology works as, for example, a software developer might. To police, the ways in which the technology *actually* functions is "black-boxed" and thus subject to specialized expertise beyond the ken of the average police officer (Christin, 2020; Pasquale, 2015; Vestby & Vestby, 2021). Think about this in comparison to a simpler technology of policing: a firearm. Police will know the ins and outs of their weaponry, when it is likely to work and when it won't, so that if their sidearm jams, they will know how to take it apart, find the problem, and put it back together again. But with AI-driven tools like facial recognition, even police do not know what is going on in its algorithmic guts—that is proprietary corporate knowledge. Of course, many of the representatives from police technology vendors with which I spoke explained that much of their job involves simply explaining to police departments what their products do and how they work, but that these demos and walkthroughs are limited to a technology's core functions and not the binary-coded ones-and-zeroes that make these tools tick. And as mentioned in Chapter 1, much like how journalists conceive of themselves as "translators" of complex knowledge about police technology who render this information digestible for public consumption, so too do the technology vendors with which I spoke. They regarded translating complex knowledge about technology as an essential part of making technology comprehensible to police, selling that technology to police, and sustaining the tool's viability within police departments after purchase.

The structures that support the purchase of police technology—namely formal procurement processes—are also instrumental in keeping those technologies a secret. As mentioned in Chapter 2, procurement is the formalized process of competitive bidding through which public institutions acquire goods and services. Public procurement will take on different forms depending on the level of government and the institution, but in Canada, public procurement is governed by a complex web of trade agreements, which impose standard obligations on how procurement is supposed to work (Canada Buys, "Public Procurement," December 13, 2023). And as was discussed briefly in Chapter 2, procurement for law enforcement may still fall beneath the ambit of these broader trade agreements, but it is by and large subject to internal policies that will vary from department to department.

Looking to Toronto policing institutions shows how these in-house procurement policies can deliberately contribute to secrecy around technology. For those hoping to do business with the

TPS, the TPS' Purchasing Unit "is responsible for procurement of all goods and services required by the organization." (*Business with the Toronto Police*, n.d.). The TPS' Purchasing Unit page highlights the unit's mandate, the trade agreements and by-laws to which they are subject, the process by which bidding on purchases works, as well as the TPS' role within the Police Co-operative Purchasing Group as part of their involvement with the Ontario Association of Chiefs of Police (even their procurement is networked). But most relevant to this discussion is that the TPS' Purchasing Unit operates under the authority of the TPSB, and more specifically, the TPSB's "Purchasing By-Law" (n.d.). This by-law exists to ensure that TPS' procurement, to quote the text directly, is "objective, fair, transparent and efficient": that formal calls to buy technology unfold in the public eye, that technologies are properly vetted and scrutinized, and that final purchases are approved through legitimate channels. This means that, sometimes, information about police technology *is* available, if you know where to look: on clunky online procurement portals,[27] or as a buried line item on a confusing budget spreadsheet,[28] or in a passing mention at a police board meeting.[29]

But the Clearview AI controversy spotlights a massive gap within TPS' procurement structures and the TPSB Purchasing By-Law, thereby flagging a concern with how cutting-edge police technology in general and FRT in particular is acquired. As I came to learn through interviews and documents, the Toronto Police, like a number of other law enforcement agencies, including the RCMP—picked up Clearview AI's FRT tool at a police technology conference as a free trial. In a report acquired through FOI by the *CBC*, entitled *Toronto Police Service Clearview AI: Usage, Review & Analysis*, submitted by TPS' Detective Operations on March 27th, 2020, it is noted that "A 'free' trial of Clearview AI was made available to TPS – [Child Exploitation Section] members shortly after D/C Davey returned from the Netherlands. ***It should be noted that the Service has never purchased any Clearview AI licenses***" (emphasis in original). Of course, free trials, by default, do not require spending police resources and public funds, so they are not subject to existing procurement rules, namely the TPSB's Purchasing By-Law, which makes no mention of free trials. This means that free trials are not subject to any of the policies or procedures that require procurement be a transparent and openly observable process. It was through this legal and

[27] See https://www.merx.com.
[28] See https://data.torontopolice.on.ca/pages/budget.
[29]See TPSB, "Vendor Award – Facial Recognition System," May 30, 2019, p. 127.

corporate structure—a structure exploited by Clearview AI—that the Toronto Police, and many other police departments, were able to keep everyone else ignorant of their use of Clearview AI. As Clearview embedded their software into investigative practice, in advance of the scrutiny mechanisms associated with formal procurement, this regulatory blind spot allowed police to use powerful, invasive, and controversial technology without an obligation to disclose its existence.

Now, procurement structures can explain why stakeholders external to policing might not hear about police technologies upon their first use, but what structures staunch the flow of information about police technologies *after* they have already been acquired? One place to look is to Canada's freedom of information (FOI) regimes. Canada's FOI regime is upheld by municipal, provincial, and federal acts that allow citizens to request timely and accurate access to internal data regarding governmental services. The TPS processes requests under the *Municipal Freedom of Information & Protection of Privacy Act* (MFIPPA), which gives individuals a right of access to information barring certain exemptions. "Under the Act, individuals may request access to general records as well as records containing their own personal information." (TPS, "Freedom of Information Request," n.d.). Appeals to decisions made at the municipal level, as well as requests for information from provincial ministries, run through the Information and Privacy Commissioner of Ontario, which is beholden to Ontario's *Freedom of Information and Protection of Privacy Act* (FIPPA). Meanwhile, the federal FOI regime is divided under two acts: the *Access to Information Act* (ATIA), which allows access to information in federal government records that are not of a personal nature, and the *Privacy Act* (PA), which grants individuals access personal information about themselves held by federal institutions (Canada Council, "Access to Information and Privacy Acts," n.d.). Access to Information and Privacy (ATIP) requests, as they are known at the federal level, is the mechanism through which individuals can access information on the RCMP.

On their face, FOI regimes are ostensibly about public disclosure. They are one of the few avenues through which academics, members of civil society, and journalists are able to access information about police technology—information which they can then relay to a public that often does not have the time or wherewithal to submit such requests. And to be sure, there is a body of scholarship—albeit a narrow one—about the importance of FOIs as data source for the social sciences more broadly and the criminological study of police in particular (Keen, 1992; Luscombe, Walby & Lippert, 2017; Savage & Hyde, 2014; Walby & Larsen, 2012).

But in the arena of police technology, FOIs often further enable secrecy, providing the legal architecture to keep people ignorant not only of police technology's use, but of its existence. A presentation for the University of Toronto's Centre for Ethics by Kate Robertson, a Toronto lawyer and co-author of the Citizen Lab's report on the police use of algorithmic technologies in Canada, mentions that there is still plenty we do not know about police technology, and much of this has to do with FOI regimes supporting this secrecy (U of T Centre for Ethics, January 25, 2022). Robertson situates this unknowing within the broader secrecy of policing and technology. She adds that we do not know *how* certain tools work, because they are still constructed in a black box (ibid.). We also do not know *whether* these tools work, as their efficiency and effectiveness are left unevaluated, or their evaluations are left undisclosed. And we do not know *where* tools are in Canada, as police are not in the practice of sharing what is in their toolbox.

Many interlocutors spoken to throughout the duration of my project shared their struggles with the tightrope walk that is Canada's FOI/ATIP regime. Academics—me included—have attested to similar challenges. Kate Robertson, Cynthia Khoo, and Yolanda Song (2020), authors of *Surveil and Predict*, noted similar barriers to their own wide-sweeping survey of algorithmic policing technologies in Canada. "Many of the freedom of information (FOI) requests submitted for this report were met with responses from law enforcement authorities that claimed privilege as justification for non-disclosure; in other cases, law enforcement agencies did not provide any records in response to the submitted FOI request, or requested exorbitant fees in order to process the request" (Robertson, Khoo, & Song, 2020, p. 2). It is tricky, then, to ever get a comprehensive grasp on how (and even *if*) Canadian police departments are using or developing other predictive or surveillance technologies, since development and usage unfolds well out of public view, and often with little desire to make the public aware. Robertson, Khoo, & Song (2020) continue:

> "Nearly every request resulted in ongoing negotiations with an assigned FOI officer or analyst. Such officers or analysts regularly sought to narrow the scope of requests, to clarify the kind of records the authors were seeking, or to seek—often exorbitant—fees for processing the request. Follow-up negotiations were pursued to address these responses where possible. Several requests received responses that asserted privilege in respect of the requested records. Obtaining records also necessitated numerous follow-up emails and phone calls, and significant time extensions were needed to fulfill the requests. In some cases, miscommunication led to the premature closing of the files, while in others, the authors would have been required to apply for fee waivers or appeal unsatisfactory responses to the relevant regulator. The authors obtained records

> across multiple jurisdictions and levels of government following such negotiations and payment of some of the smaller fees." (p. 13)

Wading into the murky depths of Canadian FOI regimes, especially when it comes to efforts to understand police technology, is, to quote one reporter who covers national security issues in Canada, "like doing a jigsaw puzzle blind-folded," or, to quote another reporter who has covered RCMP technology stories, "no exaggeration, it's pulling teeth." There are a number of challenges that make the FOI route as frustrating as it is. For one, the FOI process is, according to a Canadian reporter, a long and adversarial one: "What I tell people when I'm trying to teach them how to FOI is that the entire process is a negotiation. And so my approach tends to be to, you know, not bluff, but kind of start from a position of more than what I actually am looking for and negotiate down from there, because I know that they're going to start with wanting to release almost nothing, and then they're gonna have to negotiate up from there." Further, there is the matter of figuring out where to start; unless you have prior experience with filing FOIs or the guidance of a more practiced hand, police departments will not indicate what sort of documents you are able to request, nor is it easy to uncover information about a piece of technology if that technology itself is undisclosed and secretive. Still, Canadian reporters writing on police technology issues have come to look at FOIs as a legal tool, one that one journalist told me—if it works—"flushes out the record," getting reporters closer to that which is otherwise hidden. Many police technology reporters have even viewed their navigation of this impenetrable knowledge regime as simply a necessary part of their job; one journalist, wryly quoting Canadian musician Bruce Coburn, told me with a smile that "you gotta kick at the darkness until it bleeds daylight."

But of course, FOIs can be used as an agnotological support beam in the broader secrecy architecture. According to Luscombe and Walby (2017) and their writing about FOIs in the context of governmental practices, FOIs can be used just as a tool of organizational obfuscation and secrecy. One of the ways this plays out in Canadian policing is through exemptions. Canadian access law provides for two kinds of exemptions that allow public offices to deny people access to certain records. Exemptions under access law fall into two categories: mandatory exemptions and discretionary exemptions ("Chapter 5: Exemptions and Exclusions," *Ontario*, n.d.). Certain bits of information, like personally identifiable information, are subject to mandatory exemptions, whereby an access office must withhold disclosure by law. A discretionary exemption is one whereby the institution to which one has made a request may choose to accept or deny access to

certain records according to their own interpretations. Usually, police departments have units devoted to processing information requests, like the TPS' Information Access unit (TPS, "Information Access," n.d.) or the RCMP's Access to Information and Privacy (ATIP) Branch (RCMP, "Access to Information and Privacy," August 24, 2022), or have a government agency oversee responsibility, like the Ministry of the Solicitor General's (SOLGEN) Freedom of Information and Protection of Privacy Office, which handles FOI requests for the OPP ("Freedom of Information request," *Ontario,* n.d.). Individuals within these FOI units are beholden to access law, but are given the leeway to apply discretionary exemptions, deciding what information to disclose and what to withhold.

Provincial and federal access law states that exemptions and exceptions to access rights should be "limited" and "specific,"[30] but I argue that discretionary exemptions can be worded ambiguously to serve further agnotological ends, creating wide carveouts for keeping information and knowledge about police technology a secret. Take, for example, the FOI denial I received from SOLGEN regarding an FOI I submitted seeking information about the OPP's publicly revealed and admitted use of Clearview AI ("Request Number SOLGEN-A-2022-05436"). The discretionary denials contain wide-sweeping exemptions that were up to the institution's interpretations: I was denied access to records under s. 13(1) of the *Freedom of Information and Protection of Privacy Act* because some of the information I requested "would reveal advice or recommendations of a public servant, any other person employed in the service of an institution or a consultant retained by an institution"; under s. 14(2)(a) because information I requested would involve disclosing a record "prepared in the course of law enforcement, inspections or investigations by an agency which has the function of enforcing and regulating compliance with a law"; and under 14(1)(c), where disclosing a record "could reasonably be expected to reveal investigative techniques and procedures currently in use or likely to be used in law enforcement."

These justifications, as worded, provide police institutions with the overbroad power to stifle almost any information about police technology: the way technology is understood and contested by police could fall under "advice or recommendations of a public servant," any document pertaining to the acquisition and governance of technology could be excluded for revealing "investigative techniques," and any explanation of use of technology could qualify as

[30] See Section 2 of Canada's *Access to Information Act* (1985), or Chapter 4 of *Ontario's Freedom of Information and Protection of Privacy Manual* (2018)

"prepared in the course of law enforcement." Legal architectures of secrecy support police nondisclosure in the arena of police technology. When they work—when journalists are able to "flush out" information about police technology, or when police institutions provide a lot of information with little friction, like with my experience with submitting an FOI about RCMP's NTOP—FOI's can be an invaluable resource for disclosure.

But by and large, FOI regimes bear a deserved reputation as an unviable mechanism for learning about police technology. If academics are prevented from doing research through FOI rejection, organizational foot-dragging, or bureaucratic firewalls, then how are those beyond a select few expected to understand police technology initiatives, let alone know that they exist? A journalist reporting on justice and technology summed it up best: "Finding out that a process or system exists in the first place can be most of the battle, and then, even once you know that it exists, if you figured it out…there's still the question of 'Okay, well, how do you report on it?' Because just the fact that you know that a system exists doesn't mean that you know anything about whether it's fair, whether it's appropriate, whether the government's paying a reasonable price for it, and whether people are paying an unspoken price for that."

To sum up, architecture of secrecy that pervades the world of police technology is built on legal, political, and corporate frameworks. While some of these structures, like the under-resourcing of technological governance regimes, can be somewhat banal, other secrecy-producing fixtures can be more concerning. Emerging technologies like Clearview AI involve proprietary corporate knowledge, and vendors like Clearview have a financial interest in keeping their workings secret via NDAs. While procurement frameworks would seem to offer some transparency, as I learned in relation to Clearview AI, the "free trial" model can end-run transparency by creating an agnotological loophole allowing new technologies to evade procurement regulations. Meanwhile, the architecture of Canada's FOI regimes has broad carve-outs that police institutions use to keep their methods and uses of these technologies secret and therefore beyond public scrutiny.

The Imbalanced Politics of Transparency and Trust

Given police's recognition of their culturally ingrained inability to "sell" technology, as well as the many structural avenues through which police technology can be kept secret, the newfound premium that institutions have put on transparency comes as little surprise, especially in the wake

of technological controversy and waning public trust. However, I argue that the politics of knowledge at play within police technology can actually complicate the relationship between police transparency and public trust, and point to how one may undermine the other when police technology is at issue.

Scholars have understood transparency in governance processes to be a source of increased citizen trust in criminal justice institutions (Chanin & Courts, 2017; O'Hara, 2012; Proumbescu, 2017), and have recognized transparency principles as guiding the development of more collaborative governance practices (Gash, 2022). As a result, Canadian institutions have sought to strengthen the connection between transparency and trust in emerging governance mechanisms surrounding police technology. For one, Toronto policing institutions' AI Policy and Procedures highlight how using technology in secret can impact public trust in Toronto policing. Canada's privacy commissioners' guidance on police use of FRT says that police should implement transparency measures around their use of FRT "inform the public about FR initiatives" and "increase public confidence" in police and technology. And internal RCMP documents about the creation of the National Technology Onboarding Program view increased transparency as essential in revitalizing trust in police and technology:

> "Public trust in the RCMP was severely impacted following the OPC's decision that the RCMP violated the *Privacy Act* when it used Clearview AI's facial recognition technology.[31] This renewed the RCMP's commitment to enhance trust with the communities it serves. One way to increase trust is by increasing transparency of law enforcement's use of new operational capabilities, specifically those that involve novel collections of personal information. Very few members of the public understand how policing operations work which creates fear of the unknown. By being transparent about what capabilities are being used and how they work, people become less afraid which in turn re-instill trust in the RCMP." (p. 27 of FOI document)

Institutions have thus come to view transparency and trust as mutually reinforcing, but when it comes to police technology, police transparency efforts sometimes fuel growing public *dis*trust. To demonstrate this, one example worth returning to is the TPSB's public consultation around their AI Policy. While the previous chapter discussed this consultation in terms of police's

[31] Interestingly, there is some slippage in internal RCMP documents about which controversies are the greatest cause of public mistrust. Some documents indicate that it was the news coverage around the covert use of Clearview that first tarnished the RCMP, while other documents such as this one say it was the Privacy Commissioner's finding that the RCMP's use of Clearview AI contravened the *Privacy Act*. How police internally conceive of these controversies is fascinating and worthy of further study in other contexts.

unilateral authority to share power in the collaborative production of governance materials, this example can also be explored to demonstrate the conflict between transparency and trust in police technology.

The public consultation around the TPSB's AI Policy was designed to "create transparency about the Service's use of AI technology," but the consultation created the opportunity for Toronto police institutions to dismiss respondents' mistrust in police and technology as ignorance (TPSB, "Public Consultation," December 2021). Specifically, the TPSB shared an early draft of a forthcoming policy and invited collaboration from external stakeholders, engaging in transparent governance practices to reposition themselves as a trustworthy actor in the wake of the Clearview AI controversy. But as discussed in Chapter 2, the TPSB took umbrage with public commentary that highlighted mistrust in AI technology, mistrust of police, and mistrust of the police's use of AI technology. Some responses to the public consultation even expressed mistrust in the public consultation itself, calling it a legitimacy-seeking exercise in transparency theatre. The TPSB framed this mistrust as ignorance and used this ignorance to assert the primacy of their own knowledge over police technology and dismiss key citizen concerns.

This example shows, first and foremost, how police might undermine their own efforts of being transparent by discounting mistrustful members of the public. In this instance, Toronto police institutions are saying, 'We are the experts,' 'our technologies only work if our methods are secret,' therefore 'you just have to trust us.' Toronto's public consultation was framed as a collaborative mode of dialogue between police and external stakeholders, but as Wynne (2006) has shown, securing public trust is not a given. Wynne (2006) explains that public engagement initiatives can actually reinforce public mistrust when policy institutions fail to adopt the "frame of dialogue" in their engagement, using the engagement instead to reassert the primacy of their own expertise. Such was the case with Toronto policing institutions, who not only used the consultation to further entrench their self-regulation, but who used the consultation to claim a monopoly on certain domains of knowledge as unique to their professional expertise (Abbott, 1988; Sandefur, 2015; Wynne, 2006). This also speaks to the critiques of 'public deficit' framings of policy by public engagement, which can backfire when publics framed as 'ignorant' are

distrustful of policymakers seeking to engage the public in the first place (Blok, Jensen & Kaltoft, 2006; Durant, 2006; Wynne, 2006).[32]

To that point, the TPSB example suggests that police's attempts at transparency may be viewed with skepticism and dismissed by members of the public if those members of the public—some of whom responded to the call for consultation—fundamentally mistrust police and technology in the first place. One police stakeholder, extolling the virtues of the TPSB's public consultation, told me that that public consultation is a way "you can not only be transparent, but show the public you are trying to be transparent." But as many of the responses to the TPSB's public consultation suggest, it seems that "showing the public you are trying to be transparent" only goes so far when the public mistrusts the institution trying to be transparent and thus regards the "trying" as disingenuous.

This theme surfaced among a number of participants, who identified publics' baseline mistrust in police as a fundamental barrier to trusting the police's use of technology and the police's stakeholder consultation efforts—a mentality of "Why should the public trust the police about technology when they cannot trust the police about anything else?" A data scientist and AI ethicist involved in tech-justice advocacy, speaking about the feedback surfaced by the TPSB's public consultation, highlights how police should take public feedback seriously that expresses mistrust in policing and mistrust in technology: "…All in all, I think there's a certain amount of public misunderstanding of what AI really is and what it means. But at the same time, I actually put a lot of credence in these sorts of public responses. And it's actually these sorts of engagement with individual members of the public concerned citizens that I think should be a fundamental part of the policy itself." This individual continued that what these comments demonstrate is not so much public misunderstanding of key issues, "but rather a lack of trust with the police service, or maybe just with government more broadly. And specifically, their [secretive] deployment of technology, or really any sort of practice or policy." This individual added that this lack of trust makes sense given police's track record with being untrustworthy actors, saying that they believed "this lack of trust is accurately informed by your lived experience. And decades of history." This individual concluded by saying that what the public consultation responses reveal is less about

[32] What sets the current case apart from the public engagement discussed in these cited sources is the lack of public education initiatives on the part of police. The stakeholder consultations that Toronto policing institutions mounted around their AI Policy and Procedure were *not* accompanied by any public education efforts, and did not aspire to really 'teach' an 'ignorant' public about police technology at all.

needing to “educate” the public on how certain technologies work, “but rather to begin to rebuild that trust with the public on how this or really anything else is going to be done.” This individual’s comments highlight that transparent governance of police technology can be futile if transparent governance is built upon a foundation of institutional untrustworthiness.

Another member of a tech-justice advocacy group reiterated that a lack of trust in police and technology stands in the way of the public’s acceptance and police’s governance of technology. This individual specifically spoke to the importance of information transparency and knowledge dissemination, as well as the work police must put in to be ‘truthful’ actors, as essential to securing trust in police and in police’s use of technology:

> “Yeah, I mean, I think you're right that like, sometimes it is sort of a gap in understanding, but sometimes it's more an inability to see what the kind of concerns really are. Sometimes I think law enforcement has a hard time seeing that you've been a bad actor for—especially for certain communities—for a really long time, and you haven't been a trustworthy broker, so when you say to us, when you just promise us 'We'll use this tool, but we won't use it for surveillance. It's capable of being used for surveillance, but we won't [use it that way]," why would that community trust you?”

This individual continued by highlighting the uphill battle police have to “reckon with that lack of trust,” and how challenging it is to “bridge that gap” that opens between police and the public when police are secretive or misleading about their use of technology. This individual noted that they see potential in establishing legally enforceable requirements around police transparency about technology. Touching on issues with police’s self-regulation, this individual suggested that these legally enforceable requirements should be put in the hands of legislators and impartial government bodies, speaking to law’s prospective ability to bolster public trust around traditionally untrustworthy actors:

> “I do think, though, that's where actual policy and legislation comes into place, because I think too often police do say, like, 'Trust us' and like, you know, I don't blame them, why would you trust them? You can't take them at their word that they're...so it depends.”

Interestingly, this individual situated their discussion of trust and transparency around the use case of FRT in policing. This individual acknowledged the differences in knowledge that crop around FRT, recognizing that there is a disconnect between how police make sense of the technology and how the public perceives it, pointing to a continued controversy in public and professional discourses around AI (Ulnicane, 2021):

> "Like with face rec there can be a misunderstanding. Right now, most if not all (I'm sure there's some bad actor exceptions) but really, so far, face recognition is not used for surveillance; it's used post hoc, like something has already happened and we're actually using it to help investigate. I think a lot of people's fears about facial recognition, or what they think the harm is, is a surveillance use case where you're on the street, your face is being identified and sent to some system. And law enforcement loves to say like, 'Well, we're not using it that way.'"

But this respondent believes that police have no authority to reject or dismiss external stakeholders' beliefs about FRT, since police have historically been untrustworthy actors. "And it's like, until there's a policy that says that [police are not using FRT a certain way], until there's a law that says that, you can't ask the public to trust you because you haven't been trustworthy before." This individual used this point, once again, to vouch for taking governance of police technology away from police, in order to better broker police's relationship with a mistrustful public. "So I think that's where the acceptance of actual hard law needs to bridge that gap. It can't just be a conversation between law enforcement and the public to be like, 'trust us,' like, 'here's what the fact is,' because they can violate that trust in anytime unless there's accountability." Overall, this individual suggests that given controversies around acquisition and use, that the police have lost enough public trust that they should not be empowered to make technology-related decisions independently of public consensus.

In addition to civil society stakeholders, several of my police informants recognized this conflict between transparency and trust within their own institutions, too. These police stakeholders understood that the public was fundamentally mistrustful of the police and recognized the importance of overcoming those trust barriers. But, consistent with language from the emerging governance models mentioned earlier, these police informants regarded transparency around technology as an automatic antidote to mistrust. They suggested that transparency around technology was something that could fix police relationships with a mistrustful public.

For example, a former police officer who played an instrumental role in drafting the IACP Technology Policy Framework told me that police departments establishing their own policy around the use of police technology need to embrace transparency as an effort to break through public mistrust around policing. This individual said that "policy [around police use of technology] has…got to understand the fact that inherently the people you serve don't trust everything you say and do. So you've got to be able to be somewhat transparent in a way that still allows you to

function." Similarly, a recently retired TPS officer who served for 35 years told me that "No one trusts the cops on their own word, that there isn't a self-serving interest for what we're trying to do," but that despite that lack of trust, police should nevertheless "be more transparent" about their use of technology. These informants held aspirational views of transparency's potential to cure public mistrust in policing, but still were not able to articulate why the public should trust those transparency efforts in the first place.

So why do police departments occasionally make consequential technological decisions without keeping transparency in mind, if doing so can, as seen in justice institutions, jeopardize public trust (Chanin & Courts, 2017; O'Hara, 2012; Proumbescu, 2017)? There does not appear to be one straightforward answer, but rather a cluster of possible explanations. That same police administrator who worked on the IACP's Technology Policy Framework has a more operational and pragmatic perspective on the matter. This individual believes it to be a combination of the supposed promise technology brings as well as the lack of standards around technological acquisition and use, and the possibility of police getting so caught up in finding a solution to operational problems that they simply neglect to spread the word. "The truth of the matter" this police administrator told me, "is that most of these agencies are essentially dealing with a workflow that is extremely challenging. Enter a vendor with a way to make things better, smarter, more precise, etc. And they add it. I mean, it seems very practical. There's nothing illegal in the law that [says] 'As we understand it, we do the legal review and off we go.' Well, they didn't manage the public side of it." Speaking from experience, this police administrator suggests that "managing the public side" of technological acquisition is something of an afterthought—something that gets lost in the shuffle amid police's belief that a digital tool will fix departmental problems.

To this policy expert, police departments in North America are making things needlessly complicated for themselves by acquiring technology "under the covers." To them, a healthier approach to adopting, using, and maintaining police technology is as simple as being honest—dismantling agnotological structures through radical transparency, lack of trust be damned: "If I'm going to implement as a chief, a little community that I live in, if I were the chief…and I were going to implement some sort of AI system, that was deriving data from the traffic cameras, right. Well, I gotta be honest: I'm going to announce it before I use it." This individual maintains that active disclosure of the thought process behind the technology can demonstrate to a mistrustful public that police are taking technology carefully and thinking through a technology's

implications. Rebuilding public trust in police technology thus becomes a matter of "proving" to the public through active disclosure that police are using technology thoughtfully:

> "I'm going to talk about 'Why do we need [this particular technology]? Is there a legitimate reason that causes us to need to do work differently than we have historically?' Okay, that's met. And then the other thing I'm going to talk about is essentially, 'What it's not going to be used for,' and how I'm going to prove that to the community on an ongoing basis. 'What's the oversight? What's the quality? What's the audit trail? How does all that occur?'"

Transparency and trust are instrumental, this person adds, in thinking through technological controversy. This individual maintains that "you're asking for a problem somewhere down the road, if not immediately in this day and age, if you implement any technology without thinking through that process" outlined above. Controversy, this policy expert adds, is thus the product of police "getting caught not explaining something." This individual concludes that police have brought controversy upon themselves, and are the ones who are chiefly responsible for whatever hit to trust they take in the wake of technological controversy, because police were not as transparent as they should have been. "You should have explained it up front," they add. "You know, and to be fair, you should have had all of the leaders of that part of the city cutting a big ribbon when technology went up, you know what I mean?"

In sum, transparency and trust exist in tension within the domain of police technology. Some individuals, largely from the world of policing, regard police's present and future embrace of technological transparency as enough to satisfy a public that is mistrustful of both police and technology. This belief is supported by the emerging governance regimes at the core of this analysis; Toronto policing institutions, Canada's privacy commissioners, and the RCMP have all, in their own ways, suggested that governance that breaks open the black box of policing, tears down agnotological tendencies, and leans into more overtly transparent practices will foster greater public trust in policing. However, a number of stakeholders from the public and civil society organizations regard this as hollow, and view transparency-for-trust's-sake as unattainable given their lack of trust in policing to begin with. The result is paradoxical and difficult to unravel, but points toward something to which a handful of participants alluded: the potential value of removing police from the techno-governance equation and handing oversight of police transparency to external legislators. In so doing, efforts to render police technology transparent to the public could be more trustworthy, since these efforts will be originating not from police

themselves but from an external third party. Police transparency of technology would be imposed from without, rather than skirted from within.

The Police Technology Knowledge Playbook

Taken together, these examples of agnotology at work—the primacy of police knowledge of technology, the architectures of secrecy, and the inadequacy of collaborative structures to foster transparency around police use of technology in the face of dwindling public trust—paint a picture of what I am calling *the police technology knowledge playbook* (see Figure 5).[33] This is the first sketch of a potential model that I suggest may be useful for assessing police departments' control knowledge about their use of technology. The playbook unfolds roughly as follows:

1. Denounce public critics as insufficiently expert in professional police knowledge and practice around technology. The public is ignorant and therefore unqualified to provide input.
2. Selectively educate the public through "marketing" police positions. Conduct public engagement as advocacy work.
3. Rely on legislative disclosure and procurement frameworks to retain ironclad jurisdiction over methods, uses, and/or facts of adoption of police technology and keep them secret.
4. Then, either:
    a. Neglect public consultations, or rather consult internally, thereby concentrating police knowledge about technology within the organization and creating further gulfs in knowledge between stakeholders, which takes us back to step 1, or;
    b. Facilitate a public consultation but define the consultation narrowly around questions of acceptable use rather than overall questions of propriety of use in the first place. Reject mistrust critiques as 'ignorant,' and go back to step 1.

[33] This playbook is inspired by the *tobacco industry playbook*, outlined by public health and agnotology scholars as the techniques used by Big Tobacco to influence policy by minimizing tobacco's negative health effects (Etter, 2021; Reed et al., 2021).

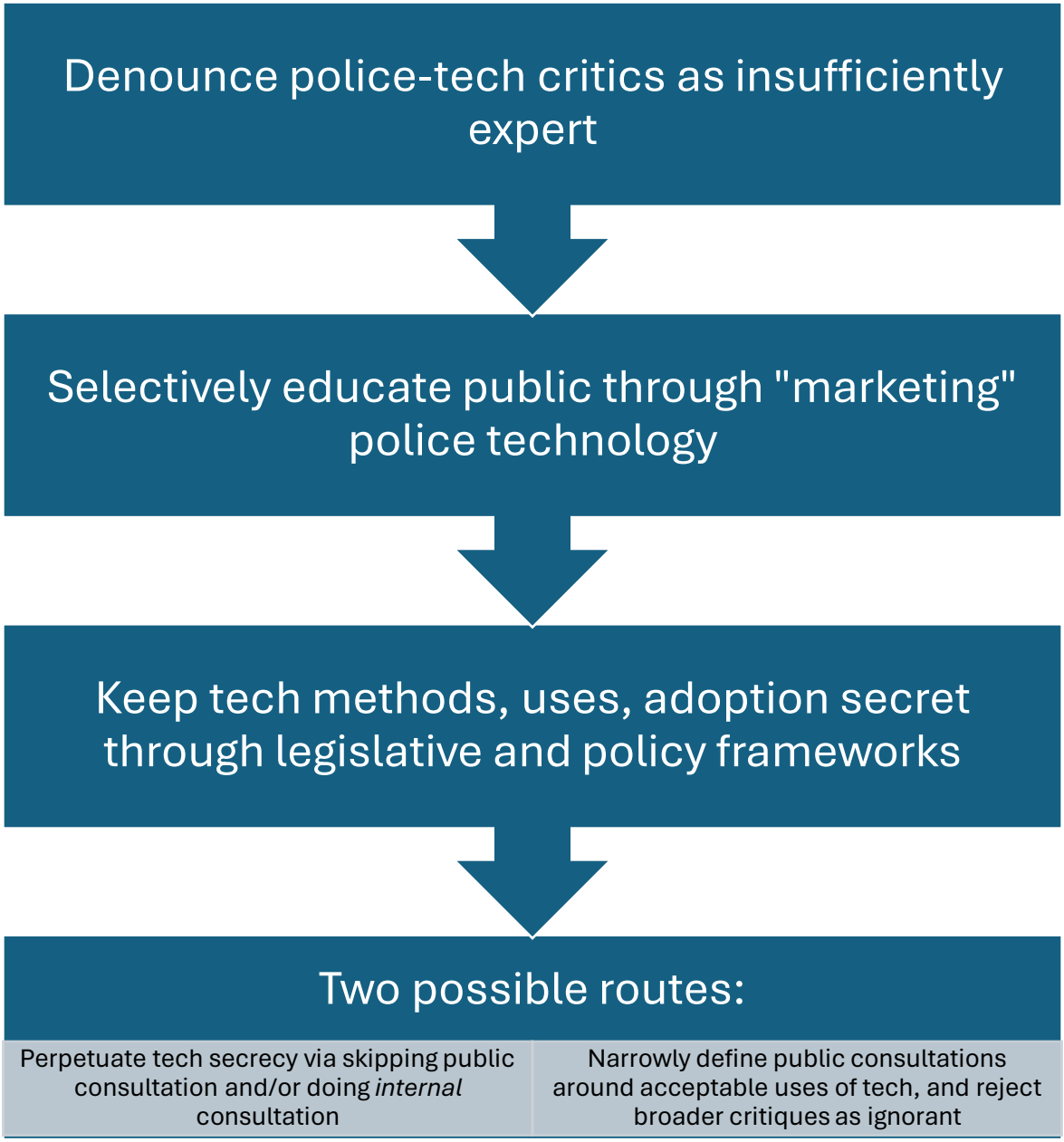

Denounce police-tech critics as insufficiently expert
Selectively educate public through "marketing" police technology
Keep tech methods, uses, adoption secret through legislative and policy frameworks
Two possible routes:
Perpetuate tech secrecy via skipping public consultation and/or doing *internal* consultation
Narrowly define public consultations around acceptable uses of tech, and reject broader critiques as ignorant

Figure 5: The Police Technology Knowledge Playbook

The three preceding examples and the playbook are early sketches of agnotology at work in police technology, and they help account for the gulfs of knowledge that stand between police and stakeholders external to police when it comes to police technologies (Barton & Davis, 2018; Bloch-Wehba, 2021; Ericson, 1989; Koningisor, 2023; Manes, 2019; Proctor & Schiebinger, 2008; Tombs & Whyte, 2003). The playbook also presents a possible explanation for how publics and other relevant interest groups external to policing come to be on the shunted side of a knowledge

hierarchy, and how this disequilibrium may contribute to mistrust in law enforcement's use of technology. Why might one expect other stakeholders and actors, dismissed by police as uninformed about the technological particulars of a digital policing tool, to understand police technologies if police withhold that information through institutional architectures of hurdles and hoop-jumps? The mere existence of this gulf—the police-made technological unknowing that afflicts stakeholders external to policing—has profound consequences, and police need to abandon this playbook altogether if they are to remove police technology and its governance from its black box.

However, early analyses of police technology governance in action suggest that the transparency-trust divide will be difficult to remedy. In the years since the ratification of the TPSB AI Framework, the sharing of the draft TPS AI Procedure, the release of the privacy commissioners' joint guidance on FRT, and the RCMP's launch of NTOP, it seems that their transparency and communication goals remain unfulfilled. The TPSB has failed to create an online registry logging the specific technologies in use and establishing a transparency portal for stakeholders external to police to access information about these tools. The TPS draft AI Procedure remains in draft form, untouched in the year since it went out for quiet consultation. And NTOP's noble transparency efforts have resulted in a program that—barring the online record of the FOI disclosure I received in November 2022—has had no outward presence, and which has fallen behind on its promise of releasing annual transparency reports. Thus, in an effort to ensure that another Clearview-like controversy does not happen again, the governance of police technology in Canada still remains a secretive, black-boxed process. How do you find transparency and accountability in cryptic, intricate, and inaccessible systems? How do you open, or peer into, the black box when its design forbids it? How do you manage the unknowable, and how can you trust what you do not understand, let alone what you do not know? Police technology can be a black box in and of itself, sure, but so long as its operation and governance is kept in the dark, and so long as regulatory artifacts aimed at promoting transparency fail, then the governance of police technology will remain black-boxed, too.

Conclusion

Knowledge is an essential yet understudied phenomenon in the study of police technology. The politics of knowledge in police technology are so consequential as to rearrange power relations

between stakeholders—differentiating between those who *know* and those who do not—and hamstring meaningful and transparent governance in the process. I argue that the attempts of the past few years to better govern police technology have not borne fruit *because* of the black boxing of governance and information. One might argue that these efforts for reform have simply lost momentum, a governance movement stalling out on what appeared to be on a transparency wave in police technology. But we can look at black boxing as a symptom of agnogenesis: the willful efforts to produce technological ignorance within others (Barton & Davis, 2018; Proctor & Schiebinger, 2008; Tombs & Whyte, 2003). None of the organizations at the centre of this project have made police technology and its governance more transparent; they have given us brief glimpses, providing draft policies or toothless guidance documents or entire programs meant to fix what the Clearview controversy revealed to be broken, but we are pretty much back where we started, with little transparency around how NTOP is working, around which departments have applied the Privacy Commissioners' joint guidance, around whether the TPS has onboarded new technologies within the parameters of board policies and a yet-to-be-finalized procedure.

For a moment there, the governance of police technology emerged from its black box, only to return to its shadowy interior shortly thereafter. To this day, we have little way of knowing whether any of these governance frameworks have been put to the test, and whether they have succeeded or failed, partly because the institutions who have created them have failed to meet most of the transparency requirements *they set out for themselves in the first place*, or because the frameworks lack the enforcement power to ensure the frameworks' actual workings are made transparent as intended.

In the final chapter, I return to the discussion of the relationship between police and technology companies, unravelling what tech acquisition actually looks like and unpacking how divergent approaches to innovation create schisms in attempts to regulate police technology.

Chapter 4: Governing Tech Where Public and Private Collide

The day's final panel now done, I head toward Exhibit Hall A for the grand opening of the IACP trade floor. This is the boys-and-their-toys portion of the conference: over 100 vendors from all over North America have set up booths, turning the hall into a shopping mall filled to the brim with gizmos and gadgetry, all available for police purchase. As I make my way through the hall, I pass the booths of companies—ShotSpotter, Dataminr—whose names I know from their reputation selling controversial, privacy-invasive technologies. I pass booths of companies—Motorola, Microsoft, Panasonic—whose names I know from their association not with public safety but with flip phones and gaming consoles and chunky televisions. And I pass companies—Fusus, Flock, FiveCast—whose names I have never heard, but who are here among the heavy hitters selling all-in-one surveillance solutions to law enforcement.

Then I pass the booth of a company whose name I know all too well: Clearview AI. What baffles me, though, is the simple question of how they are here at all. Judging by the reps' gladhanding a steady clip of visitors, you would never imagine that Clearview AI had just recently lost a lawsuit brought by the American Civil Liberties Union for violating the Illinois Biometric Information Privacy Act (ACLU, May 9, 2022). Nor, for that matter, would you ever guess that Clearview had just gotten slapped with a $10 million fine by the UK's Information Commissioner's Office for violating the country's data protection laws (Heikkilä, May 24, 2022). And this certainly could not be the same company—operating so carefree, still handing out free trials—that had been deemed illegal and forbidden from operating in Australia, parts of Europe, and Canada (EDRi, April 6, 2022).

My time trawling the IACP Technology Conference's exhibit hall highlights the obvious: at the end of the day, the world of police technology is still a business. Police are buyers and technology companies are sellers. Seeing Clearview AI's booth shows that the technologies that ignite so much controversy, even the most privacy-invasive ones, must come from somewhere, legal consequences and regulatory fines be damned. It also suggests that law enforcement may not have learned their lesson the first time: police are still eager to acquire problematic tech, so much so that they are not put off by the risk of doing business with companies as (seemingly) blackballed as Clearview. Clearview's presence in the exhibit hall, at a conference where panelists were even afraid to say the company's name, is further cause for reflection on the curious nature of the vendor-customer relationship in police technology. This relationship remains an understudied

aspect of scholarship on both policing and technology. The intersection of order maintenance and capitalism is well-trod scholarly terrain (Forst & Manning, 1999; Spitzer & Scull, 1977; Van Steden & Sarre, 2007), and there is burgeoning literature on the role that surveillance technology companies play in driving police policies (Crump, 2016; Joh, 2017; Manes, 2019). Still, the economy of police technology is an area worthy of further inquiry that represents a fascinating cross-section of public and private interests. To quote a public sector consultant and researcher with an expertise in police technology, "Public safety tech has always been private."

This chapter explores the consequences of this collision between public and private sector interests and its implications for the governance of police technology. First, this chapter provides a look into the complicated sales process that technology vendors navigate, but from the perspective of technology vendors themselves—something that has heretofore been lacking from academic scholarship on police technology. Then, it unpacks the tensions that arise between vendors and police in the former's attempt to offer solutions to law enforcement and the latter's attempt to innovate for the sake of improving public safety. I argue that when it comes to police technology, Canadian police departments appear caught between two worlds. The contentious public-private partnership that emerges when public sector organizations like the police try to buy a private company's product proves sticky terrain to navigate. As a result, the regulations of public organizations occasionally clash with the cutting-edge expectations of private enterprise. I argue that police use of advanced technology thus puts their regulatory identity in crisis: police wind up caught between the rule-bound bureaucracy of the public sector and the move-fast-and-break-things ethos of private enterprise.

The Business of Police Technology

This section explores what the police-vendor relationship looks like and how technologies get into law enforcement's hands in the first place. Previous chapters have talked about some of the circuitous and gap-riddled routes that technology has appeared—sometimes without obvious explanation—in police departments, namely through procurement-rule-flouting free trials at police technology conferences. But here, it helps to ground the analysis in what the police-vendor relationship looks like under normal circumstances to better understand how it can go wrong. The police-vendor relationship involves more than just the police and the vendor; rather, it involves a bevy of other actors and groups who vendors have to navigate differently in order to successfully

sell their product. The success of a sale, I suggest, is often dependent on how well police can collaborate with vendors, and how well vendors can collaborate with external stakeholders.

At the heart of the police technology business is, as has been discussed in earlier chapters, procurement. When it comes to spending public money, there are a series of touchpoints that guide the process. And when it comes to police technology, there is, to quote a civil society advocate with expertise on police technology, a template: "You hear about it, you think about it, you examine it, then you procure it." This is not all that different from other public spending, but it poses interesting challenges for policing and their use of cutting-edge technology. When things are done properly, there are a set of standard processes through which police technology makes its way into departments.

I spoke to representatives from ten technology vendors, all of which recounted the very similar journey their products take throughout the police-tech-business pipeline. One of those representatives, an individual with over 20 years of experience in public safety technology who currently works for one of the largest police technology companies in the world, recounted this process to me in vivid detail. It is worth sharing their comprehensive response in their own words because they chart, in meticulous detail, a process that has otherwise not been documented in the police technology literature, and which is better explained by the professional who does this for a living. Even though this representative speaks specifically about their experience at their current vendor, they often generalized their experience to past experiences working for other vendors in the police technology space, and provided insights that were consistent with those of the nine other vendors with which I spoke.

When asked about the "common path" technologies take on their journey into law enforcement's hands, this representative told me that the process will usually begin with police identifying a particular problem:

> "The most common path is we have discussions with some member of the command staff regarding a [crime] problem in a community. That conversation could be them reaching out to us. That conversation could be us reaching out to them. That conversation could be more of a reference scenario where one of our chiefs who has [technology name], spoke to one of his peers and shared with him some of the successes. Those initial discussions can come in a variety of ways. But there's typically some initial discussion regarding, 'We got a problem, I need to understand more about what your technology can do to help us.'"

Once the police department has identified the problem and the vendor whose technology can solve it, it falls to the vendor to show off their tools to an emerging network of relevant actors with a stake in funding the technology's purchase:

> "We will go through a series typically of presentations and demos, often involving the chief command staff. Some cases that may involve some elected officials, it may be a representative from the mayor's office or some city council people."

During the presentation and demo to the network of stakeholders, the vendor starts by "helping them understand" the way the technology works and how it is the right solution for the particular problem as identified. Most important, the vendor establishes the parameters of their police-vendor relationship, and emphasizes that this relationship must be collaborative if the technology is going to work as promised:

> "So we talk a lot about community engagement, community trust, and what they're going to have to do in deploying our system, because the reality is, our system is only as valuable as the response protocols that the agency puts in place, and how they respond with the [specific type of crime] intelligence information we're now making available to them. And so we'll put a lot of focus on the role they're going to have to play in the way the response protocols that they put in place to deal with this information."

This representative clarified that though "the underlying message, the key elements in the message are the same, regardless of the audience," there are some aspects of the presentation and demo that are variable. Depending on who is being presented to, the approach to demoing the technology might change, suggesting that these presentations are tailored to different stakeholders and the vendors' imagination of what would be most persuasive to them. For example, when "talking to command staff":

> "…we're probably going to spend more time talking about what this means to the officer. What this means to the detective. What this means to the situational awareness and arming them with more information to respond, but do so safely, to know what they're stepping into. And what it's going to mean from an investigative standpoint in terms of evidence collection, being able to interview witnesses, and arrest the perpetrators."

Compare this to the more victim-centric approach the company uses when directing their presentational demos to government and civil society actors:

> "When we're talking to elected officials, community groups, community leaders, we're probably going to, again, talk about same stuff, the same value proposition, but we'll very likely spend more time focusing on what this means to the victims, and what this means to the citizens in that community where 911 is no longer serving them anymore, and we're there to pick up where 911 leaves off. And the reality is they deserve the same kind of police response that the most affluent neighborhoods are going to see and expect, but they're not going to get that if they rely solely on 911. So we spend more time emphasizing more in terms of what it means to the local community."

Assuming all goes well at the demoing stage, the next step involves the vendor and department working their way through the procurement process. Even though procurement systems are set up to be competitive and democratic, most procurement systems create carveouts that allow police departments to only seek the product of *one* company, if what that company provides is a unique technology that no other companies produce:

> "In most cases, if they elect to move forward, we—in probably 90 plus percent of the time, we move forward in what is referred to as a 'sole source procurement.' Their Purchasing [Department] is obviously wanting to make sure that if there are multiple vendors, they can offer the technology. Everybody's given an opportunity to what is typically a 'RFP,' Request For Proposal process. But if they find 'Well, we're going to spend the next six to 12 months going through an RFP, and the reality is, there's only one company that can do what needs to be done here,' then they can, in many cases, waive the RFP process and go through what's called a sole source procurement."

One hurdle that can arise during the procurement of police technology is the question of whether a department has sufficient resources for tools that might be innovative or beyond the traditional, baseline work of police departments. To overcome this hurdle, police technology vendors may be able to assist in developing funding networks to bring their innovation to a particular agency, involving collaboration and resource-sharing among other stakeholders:

> "In some cases, the challenge is securing funding. For computer-aided dispatch, or a 911 system, there's a line item in the budget. There's a line item in the budget for a lot of those mandatory core software applications. When we go into a community for the first time, there's often not a line item in the budget, right. So that's why some cases, these involve some presentations to elected officials. We may assist them in

> identifying grant funds that are available. We may assist them in helping establish some sort of public-private partnership of various stakeholders in the community. We may present to some legislators a variety of things we can do to assist them in building a case and securing funding for them."

A key part of securing resources involves drafting a proposal and making a "business case" for the tool in question. The technology vendor may have to present this business to any number of stakeholders, depending on how many actors or groups are involved in approving police purchasing decisions:

> "That typically is the cornerstone of producing a proposal, a financial proposal that defines what we're going to do, where we're going to do it, and what the annual fees will be for establishing that type of subscription service. We do everything software as a service, so there are some one-time fees to set up our system, some onboarding fees, one time. And after that, everything that the customer may need is handled through annual subscription. So we'll present a proposal. That proposal may involve going to city council, or the county board."

In stating the business case and fleshing out their proposal, vendors need to present a coherent vision for how the technological project is to be executed, and what problem it sets out to address. This is usually done in collaboration with a number of technical actors within police departments:

> "We will go through a process of evaluating their [specific crime type] data and establish a coverage area. We want to be where we're needed. We don't want to be where we're not needed. And so we'll work with him looking at [specific crime type] data and identify a coverage area, and work with them to define the right boundaries around that coverage area. We have people on our team that are analysts that'll analyze the data. We're typically working with somebody in command at the police department or sheriff's office, and often an analyst their team may be involved. And we're looking at where we can provide value and what the coverage boundary should be around that area."

Finally, once the proposal has gone through revision, vendors must get other stakeholders on board, once again showing the importance of collaborative and network arrangements in hashing out the above-board sale of technology to police:

> "Now, it's about getting political support, funding support. Typically, we're talking about expenditures that require City Council or County Board approval. We may assist

> in presenting the city council, we may assist in helping them present to city council. It varies agency by agency, what role they want us to play, but very often, we're involved in helping them build their business case. Once it is approved by city council, we're then moving into contract negotiations. We're working typically with a city legal department procurement and hammering out the terms of the contract. Sometimes that's done before city council or county board approval. Sometimes it's after—it depends on the agency. But we'll hammer out a contract, and once everything meets the requirements of both parties, then we execute that agreement. Soon after we execute the agreement, then we have a project kickoff meeting, and we start the process of deploying the system."

The birth of technological innovation in policing can be understood as a sociotechnical system (Borrás & Edler, 2014): a multi-group, multi-actor process that takes into consideration social dynamics between stakeholders, economic resources available in jurisdictions, and the specific political contexts of cities and neighbourhoods. Technological innovations are, to the police and to technology vendors, positioned as responses to specific problems, and are developed in governance networks comprised of actors and interest groups from local government, police departments, and the community at large. It is a cumbersome process, and a complicated one, but one that a large technology vendor such as the one to which this representative belongs are uniquely positioned to handle: being as big as they are, they can support themselves through the drawn-out and intricate processes of establishing connections with stakeholders and navigating tricky procurement infrastructure to bring technological innovations to the thin blue line.

The Challenge of Public-Private Innovation in Uncertain Regulatory Space

Of course, what the sales rep outlined above is what happens when technological innovation goes according to plan. But in my discussions with individuals from policing, technology companies, and civil society, there are challenges that emerge from police technology's position at the intersection of public and private sectors and the regulatory questions that arise within—questions which make innovation uncertain and unviable.

a. Innovation and Regulation at Odds

In seemingly every industry, regulation and innovation are often pitted against one another. Innovation and regulation are seen as either incompatible, mutually exclusive, or as needing to be reconciled for one another's sake (Aghion, Bergeaud & Van Reenen, 2023; Knut, 2016; Paraskevopoulou, 2012). One of the most common refrains within discourse around the

intersection of technology and governance is that technological innovation far outpaces any attempts at containing it (Aspray & Doty, 2023; Cino, 2017; Hagemann, Huddleston Skees & Thierer, 2018). This rhetoric dominates cultural and political conversations whenever cutting-edge technologies eclipse the courts, like how the advent of cellphones and sexting forced consent laws to play catch-up, or how digital piracy of copyrighted media created challenges for all-of-a-sudden outdated intellectual property legislation. As a result, 'innovation' has come to bear connotations of private-sector ingenuity, while 'regulation' bears the connotations of rigid stick-in-the-mud bureaucracy and of a meddling public sector.

This rhetorical theme of technological innovations outpacing regulation is common within the realm of police technology, too, and appeared frequently in interviews across stakeholder groups. An expert from the world of advocacy, speaking about the RCMP's disagreement with the OPC on the OPC's ruling that the RCMP's use of Clearview AI violated the *Privacy Act*, told me that they were skeptical of the police's argument that using FRT was not against the law, because this justification "beg[s] the question of whether law is adequate in any way." The RCMP's claim that there are no privacy laws that forbid the use of FRT, this stakeholder added, forgets the fact that "our laws were written at a time when files meant something in a folder." Several journalists who covered the Clearview AI controversy and Canadian police's acquisition of concerning technologies pointed out to me that part of what accounts for how controversial these tools are, and part of what makes this technology what one reporter called "a moving target," is the lethargic governance backdrop against which these tools are situated. In speaking about how law cannot keep up with police technologies' effects on civil liberties, one journalist jokingly referred to policing's technological innovation outpacing law and policy as "like a race between Usain Bolt and a turtle."

These concerns also arose within police institutions. The individuals from RCMP's NTOP with whom I spoke mentioned that "the fact that these technologies are always changing, and there's not a lot of settled case law on many of these very new emerging technologies," posed the greatest challenge to creating a new governance regime to regulate the RCMP's technological innovations. Many individuals from privacy offices across Canada, in talking about the joint guidance they created on using FRT, specifically said that when it came to regulating police technologies like FRT, that they were always "playing catch-up" or struggling to "stay ahead of the curve," as they put it. The guidance on which they collaborated, they said, functions as a

bridge—albeit an unenforceable one—between outdated privacy laws and new technological developments. One individual who actively drafted the FRT guidance pointed this out to me, saying that "the law is, like, 20-30 years old…so it doesn't say, 'When you implement facial recognition technology software, you have to do X and Y and Z,' right?" In further highlighting this legislative lag, this individual added that the privacy offices supplemented their joint FRT guidance with a statement proposing a new legal framework for governing police use of FRT to specifically call out and call on the Government of Canada to modernize what this individual referred to as "deficient" legislation.[34] A participant from an advocacy organization in Ontario used this gap to extoll the virtues of moratoria: certain jurisdictions in the United States have responded to instances where police have used FRT "because there's no law against it" by imposing a moratorium on FRT until law can catch up. This individual was baffled why Canada had not responded to the regulatory uncertainty around FRT by imposing similar moratoria of their own, despite continued calls to do so from government and civil society.[35]

But making sure that laws are caught up was not always top of mind for my participants, who occasionally viewed law and technological change as borderline irreconcilable. In a conversation with an individual responsible for drafting the TPS' AI Procedure, I was told that governing AI in policing is so difficult because police are constantly wondering how to "deal with all these questions in a flowing form that won't stymie progress." They added, "We want to be innovative, but we don't want to slow everything down." When I pressed this individual about whether being innovative is worth "going fast," they relented a bit, telling me that police "have to have a thoughtful process" for acquiring and using technology if they are going to innovate safely. When I ultimately asked this individual about the timeline for when the formal Procedure would be finalized and implemented, I was told, "As soon as possible, but as best as possible," suggesting that good governance takes time, but that time is still of the essence if police are to innovate at the level they desire.

[34] Another privacy professional got existential when I asked them about police technology outpacing law: "I find that almost gives me intellectual vertigo sometimes where it feels like the world is almost increasingly complex, and the systems we have for dealing with things I don't think have scaled to match. And that kind of terrifies me, but as a human." Heavy stuff.

[35] For more on this call for moratoria, see the ETHI report, "Use and Impact of Facial Recognition Technology" (Kelly, 2022), as well as advocacy work from the Right2YourFace Coalition of which I was a member as part of my time at the Canadian Civil Liberties Association (https://right2yourface.ca, 2023).

Representatives from technology vendors who work with police told me that despite this desire, police simply lag well *behind* other industries when it comes to technological innovation. Part of this lag, I was told, stems from whatever pre-existing technology a police department is working with. Oftentimes, I was told, police's digital infrastructure had calcified into part of the furniture, further constraining technological development (Hughes, 1987; Hughes, 1994; Hughes, 2000). One participant even told me a story of how he and his start-up's co-founder had to "backdate" their data analytics tools to accommodate a police department that was still using Windows 7 as their operating system. Further, I was told that vendors were often restricted by human and financial police resources. "If you go to a 10-person agency in South Alabama or Nowhereseville, Canada," I was told by a sales rep from a vendor that sells in-car police computers, "their budgets are probably super tight." This, the vendor added, would grind innovation to a halt, and would force vendors to have to "get creative" if they were hoping to equip a slow-on-the-uptake department with gadgetry. Thus, much like the previous chapter's discussion of how police resources can hinder technological transparency efforts, technology vendors told me that limits on police resources can be a similarly frustrating factor impeding innovation.

Conversations with other stakeholders suggested that besides old tech infrastructure and shoddy police resourcing, police simply could *not* innovate as quickly as they would like, and that this issue was primarily one of police culture. In speaking with individuals across stakeholder groups, I glimpsed a police culture divided into factions: those who wanted to push Canadian policing's technological capacity forward, and others whose adherence to strict occupational culture made them resistant to organizational change (Chan, 1996; Skogan, 2008). One Chief Information Officer (CIO) from a police department in Ontario—who described themselves as a "project management professional" in charge of technological initiatives in policing—told me that those who adhere to policing's reluctant organizational culture oftentimes hamstring innovation:

> "And if you look on this maturity model, we are considered a trusted operator: we fulfill work orders, we support functional business applications, and we have reliable service management. [But] when you listen to me talk, and I talk about wanting to move forward and be this business partner—effective execution on business projects, strategic use of analytics and customer technology—this is where we want to be, but we keep on getting reined back, and I feel it's part of the culture of the organization. I can try and improve my maturity level of my department, but if the organization culturally isn't there, ready to catch the ball, you're kind of reined back a bit."

This CIO continued, saying, "When it comes to technology [in policing], I think people look at technology and think that technology is going to fix all of their problems. The reality is that technology can do anything provided you've got a solid direction and process." 'Direction and process' are important, they continued, because they serve as the governance frameworks that structure and steer the proper use of technology in policing and which place parameters and guardrails around defining acceptable technological innovation within departments.

However, this CIO concluded, getting people on board with new processes is often a struggle. "Policing is a very old institution," they tell me. "When you start trying to change, things kind of get a little messy, because it's like 'What do you mean, I need to change?' … You can have the best technology in the world, but if you don't have solid process, then it's all for naught, and you see a lot of projects failing." Here, it is a lack of clear regulatory processes and governance frameworks—coupled with policing's well-documented resistance to change—that makes technological innovation an unachievable enterprise. Police, participants kept telling me, *want* innovative technology, but the uncertain regulatory space and stubborn occupational culture can preclude it.

In speaking with stakeholders on the business side of police technology, it often appeared as though there was no winning when it came to technological regulation in policing: no regulation and innovation becomes impossible, but too much regulation and police cannot innovate. The founder of a police technology start-up told me, for example, that finding the most productive trade-off for regulation and innovation was "a fine balance to try and hit." They added that too many governance mechanisms—such as rigorous approval processes, evaluation criteria prior to acquisition, ongoing monitoring requirements during a technology's use, and transparency standards throughout the entire technology acquisition and deployment process—"definitely would put another hurdle in the process for adoption." One representative from another police technology vendor referred to this as "the procurement barrier": the onerous nature of procurement regulations that make it harder for police technology companies to sell innovative tools to police departments.

These mentions of "the procurement barrier" pointed to a central tension hindering innovation in police technology: the tension between the more permissive business models of the private sector and the "over-stringent" regulations of the public sector. In speaking to technology vendors, police technology consultants, and police administrators, I was told that, traditionally,

technology companies are funded by venture capitalists. These venture capitalists were often willing to provide external funding to technology companies on the basis of their belief in that company's future success. This external funding, premised on venture capitalists' estimation of a technology's upward potential, would then allow vendors to develop their technology. This funding would also support vendors while they tried to make sales, providing a stable financial cushion to tech companies as they worked their way toward profitability.

But, I was told, there is a fundamental and obvious difference between the two sectors: the public sector in general and law enforcement agencies in particular are, by their nature, more "risk-averse" than private enterprise. A representative from one technology vendor told me that unlike traditional private sector funding relationships, vendors cannot rely on "police services to give you enough money so that you can build" a tool for them. Because police are risk-averse, and because they are spending public funds through procurement processes, they want tried-and-true technological solutions, and are less inclined to take a gamble on unproven innovation. This was corroborated, in part, by two individuals from a unit within the RCMP devoted to modernization, who told me flat-out that "advancing big technological change in the RCMP has always been a challenge" due to public sector governance models that impact "how we go about setting priorities and assigning money to these projects." To that end, the police technology vendors with which I spoke suggested that police were by no means as innovative as they were perhaps making themselves out to be. The innovation-driven mindset police had adopted toward technology was undercut by the experiences these vendors had while actually working with police agencies—agencies that proved to be frustrating to work with by dint of their risk-averse public sector trappings. One Canadian police consultant said it best when they told me that even though police are often drawn to "the shiny object" of technology, the police "institution is not, by default, a test lab for innovative, bleeding edge technology": "Very rarely do the police articulate the need for the shiny object, engage in innovation to produce the shiny object, and then step up and put its hand in the air to pilot the shiny object."

Interestingly, many within the tech sector—from representatives at tech companies to police technology consultants—qualified their characterization of police as especially "risk-averse" to what they referred to as "smaller" police technology vendors. Many of those in positions at smaller technology companies ("smaller" being based on the number of people who work there and the amount of market impact they have made in selling their product to law enforcement)

decried a regulatory system that decidedly works against them, a system that favours established companies at the expense of 'the little guy.' "Police services don't want to risk working with small companies," one CEO of a police technology start-up told me. "They put out bids for projects, and they're expecting companies that are large, [like] Axon," referring to a company with its own monopoly on body-worn cameras and digital evidence management in Canada. The main reason that police wind up as averse to working with smaller technology companies, and the main reason behind why "you need to be big to sell into this industry," as one vendor told me, is because bigger companies have more resources to survive and support themselves during long and burdensome procurement processes. These smaller police vendors view the deliberately slow procurement cycles of the public sector as concerning, and entering into one of those cycles with police "[is] gonna just kill all the little guys like us."

These long and burdensome procurement processes hit smaller tech vendors the hardest. Speaking from experience trying to navigate the complex terrain of police departments in Ontario, one representative from a small technology vendor that provides police with data management software told me that, "It takes a very long time to sell," before regaling me with a horror story of a colleague at *another* small technology company that was three years into a seemingly never-ending procurement cycle selling their "niche application" technology to the Toronto Police Service. An individual who worked as a technology reformer for an Ontario police department corroborated this, telling me that though they would "love to work with start-ups" and smaller technology companies, the way that police procurement works means that smaller companies "are not likely to be able to put together a hundred-page reply" to a request for proposals, and that "they're not going to be able to structure things financially in the way that [police] require." This police administrator added that public sector procurement processes are regulated in such a way so that they remain "stable" and so that police agencies are not "burned" by spending "a ton of money [on technologies that do not] lead to anything." This focus on self-professed regulatory stability aligns well with what a representative from a Canadian company that makes 911 alert management systems said about police's risk aversion: "There's a reason why 'police tech' is not really a thing…and that has to be because of how police services think: they don't have an innovation mindset, or a trial mindset or 'Let's try this and see if it works. Let's try that.'" This vendor's characterization of "how police services think" conflicts with how some police might think about themselves, and points to police's technological identity being in crisis: to some police

administrators steeped in private sector jargon, police think like innovators, but to vendors, police think like the risk-averse public sector actors they are.

Beyond their specific gripes with prohibitive procurement processes, participants in the world of tech spoke of broader gripes with the public sector's tendency toward over-regulation. Some were concerned about what public sector transparency requirements would do to small police technology vendors. These participants suggested that public sector standards to make a vendor's technology more auditable, more easily monitored, and more transparent could impede hinder innovation as smaller technology companies would not have the resources to meet such stringent expectations. "Like imagine there's a regulation on online reporting," one tech vendor told me, "that you have to have analytics, and how many [data points] come in, and how many of it is biased, or something like that. We wouldn't even get a start, right?" Participants like these suggested that some police technology vendors simply lack the resources to be as transparent as the public sector requires, and that this would be sufficient to hinder certain companies' ability to help police innovate.

Yet another example of supposed public sector over-regulation was the public sector's embrace of layered and collaborative governance models that some argued restricted innovation. In my conversation with a technology consultant who works with police departments across Ontario, I was told that public procurement processes are obviously part of the problem, but that the real culprit slowing down innovation in policing was a public-sector governance model that forced interconnectedness of stakeholders. This individual told me that unlike the private sector where there are fewer decision-makers and fewer barriers between a technology vendor and a buyer, the regulatory mechanisms in the public sector world of police technology require that "you have too many stakeholders" who have to "build and reach consensus." In working as a private sector actor within a public sector model, this police technology consultant highlighted their distaste for the public sector ways of acquiring and implementing new technologies. To this individual, public sector governance regimes that brought "too many cooks in[to] the kitchen" contributed to what this individual referred to as "an issue of a lack of innovation, lack of being technical": since these multi-stakeholder efforts often meant police technology projects failed to materialize, they were, according to this consultant, the reason "police were kind of always behind in technology." This suggests that multi-stakeholder modes of networked and collaborative governance can actually prevent police and technology vendors from achieving the collectively

sought goals and objectives that these theories emphasize (Ansell and Gash 2008; Emerson, Nabatchi, and Balogh 2012; Ran and Qi 2019; Wang & Ran, 202).

With that said, some viewed the collaborative, multi-stakeholder nature of the public sector as a plus. One individual who worked as a technology reformer for an Ontario police department described the collaborative and consultative set-up of public sector innovation efforts—in particular the ability to bring in outside consultants—as a productive way to get police out of their "echo chamber." By "bring[ing] in extra [human] resources…who are skilled up in certain new technologies," this police administrator told me, consultants are able to "engage in knowledge transfer," so police looking to innovate technologically can get the benefit of diverse perspectives and expertise. But by and large, most participants who made mention of multi-stakeholder involvement in police innovation conceived of the overabundance of stakeholders as having counterproductive and restrictive regulatory influence—a 'death by committee' mode of governance mentioned above that ensnared innovation in bureaucratic limbo.

Amidst all the commentary from stakeholders about the mutually reinforcing struggles that regulation and innovation create for one another within police technology, a handful of participants pointed to the lags in both innovation and regulation in a way that surprised me: by describing these lags as for the better of policing and society. A representative from a police technology vendor told me:

> "…There almost should be a lag in a sense because a service that society considers to be critical, like policing, shouldn't adopt bleeding edge tech, because there's always problems with bleeding edge tech, and if they adopt technology that has problems, then that's going to disrupt the stability of what we consider to be core services. … It makes sense and it is reasonable for them to be more cautious when adopting new tech because it has a larger threat on what their core operation is."

Another participant, an AI safety expert and advocate, framed this issue in similar terms, saying that police view technological innovation as "a way of increasing efficiency of the police force, which means…making police an even more blunt instrument of force." Under-regulated technological innovation in policing, this individual suggests, could be a worrisome gambit, as 'optimizing police services' simply means police adopting more and more technologies that further consolidate and exacerbate expressions of police power. These participants seem to suggest that over-restrictive public sector rules on innovation—rules that make it *harder* for police to get

technology—are thus essential for minimizing the harm that this technology can have on the police and the policed alike.

Of course, some stakeholders within policing highlighted a crucial problem to the lag that overregulation creates: the possibility for police to sidestep regulatory processes. For example, internal documents speculate on a potential flaw in the National Technology Onboarding Program's aims of centralizing the evaluation and acquisition of technology in the RCMP. According to this document, "the intensive NTOP assessment process will inevitably slow down the procurement and deployment of operational capabilities," leading to "a decrease in client motivation to engage with NTOP" (A0764529, p. 49). The authors of this document hypothesize that the regulatory burden of NTOP is actually a "barrier" that RCMP members may wish to go around. The "intensive NTOP assessment process" may actually undercut the Program's reason for existence: it may deter RCMP members from bringing their technology to NTOP at all, encouraging them instead to skirt the burdensome governance structure that NTOP imposes. But even if this is a possibility, the participants who spoke of overregulation's benefits for impeding potentially risky bleeding-edge tech raise a noteworthy point: that subjecting police technology to overly burdensome governance is better than the harms that may ensue from not subjecting it to any governance at all.

But oddly enough, *not* subjecting technology to any governance at all can, in its own circuitous way, actually *have* a regulatory effect on police technology. Specifically, participants and internal documents have revealed that the legal ambiguity around FRT has by and large brought FRT's use in Canadian policing to a standstill—a sort of regulation in regulation's absence.

In an FOI disclosure from the Office of the Privacy Commissioner of Canada, minutes from a 2021 meeting between then federal privacy commissioner Daniel Therrien and president of the Canadian Association of Chiefs of Police (CACP) Brian Larkin quote the CACP as claiming that "police agencies are generally waiting on further direction (policy, regulation, guidance, etc.) before implementing FRT" (A-2022-00057, p. 199). Further, a representative from NTOP told me that in the absence of clear-cut law around FRT, most police in Canada have simply opted to "turn it off," shutting down their use of the technology for fear of inciting further controversy. This was similarly echoed by the founder of a police technology start-up in Ontario, who told me that the lack of governance around FRT, as well as technology's continued source of controversy, have

put fear into technology companies and police departments alike. “A lot of start-ups now, they don’t want to do anything to do with facial recognition,” I was told. “Some of the conferences I've been to, the companies and integrators, they're like 'We're waiting.'” This individual added that companies and police agencies are “waiting to see what the regulations are.” “Or like, 'maybe when things cool off, then we'll start it,'” they added, referring again to FRT’s status as a scandal magnet, “but for now,” this individual concluded, “everyone’s just waiting.” Thus, the regulatory ambiguity around FRT seems to have had more of a regulatory effect than laws or policies ever could: it has steered some Canadian police away from the technology altogether.

Overall, police’s use of technology in Canada is defined by shifting tensions between innovation and regulation. As cross-sectoral stakeholders have told me, many members of police organizations desire “the shiny object” of technological innovation, even adopting the language of private sector innovators to prove their cutting-edge bona fides. But police departments ultimately grapple with innovating in a way that is satisfying to themselves and to others. Resource restrictions and a change-resistant police culture account, in part, for slow technological innovation, but much of what throws wrenches in innovation’s gears are the conflicts emerging from policing’s “risk-averse” public sector identity rubbing elbows with the move-fast-and-break-things ethos of the private sector. The burdensome procurement cycles[36] and multi-layered approval processes of public sector governance proved to be barriers to police technology companies, who regarded these public sector features as slowing down technological innovation while making police all the more challenging to work with. In sum, analyzing technological innovation from the side of both police and the private sector highlights how over-regulation and under-regulation exist in perpetual states of contradiction. Over-regulating police technology can hinder technological innovation, but as is the case with NTOP, it might also encourage police to simply use technology while sidestepping burdensome regulatory regimes. Under-regulating police technology can facilitate innovation, turning police into an “even more blunt instrument of force,” but as is the case with FRT in Canada, it can scare police off, preventing them from using contentious technology in unregulated space.

[36] This provides an interesting contrast with previous chapters worth further exploration: unlike earlier discussions of how Clearview AI’s FRT free trial allowed police to sneak the technology into their departments undetected, vendors who spoke of navigating police’s procurement process through more conventional avenues found the process to be a barrier to getting technology through the door.

b. The Encroaching Private Sector on Public Police Technology

This conception of police as ineffective technological innovators is somewhat ironic given what I argue to police's absorption of private sector modes of speaking about, administering, and governing technological innovation.

Many police administrators have adopted the jargon-heavy corporate speak of private sector innovators, suggesting a public sector actor trying on the private sector's clothes to fit in. Returning to a quote mentioned above from my conversation with a CIO at a Canadian police department, I was struck by how this individual described themselves as a "trusted operator," and how they described their work as "fulfill[ing] work orders" and "support[ing] business applications." This police CIO also spoke proudly of how they helped their department hit "maturity model" benchmarks that proved they did "reliable service management" that "effective[ly] execut[ed] on business projects [through] strategic use of analytics and customer technology." The adoption of private sector language to speak of police technology operations hit its peak when this CIO frequently referred to the community that their police department serves as "the customer." This, I suggest, is emblematic of a public sector organization coming to think like private sector actors given the blurry public-private boundary that police technology straddles.

This managerialist vernacular is encroaching on the development of police technology governance models, as well. A program description of NTOP, found via FOI, states that one way to motivate policing units within the RCMP to participate in the NTOP process is by "creating a strong client service model and fostering positive working relationships with clients," using the "clients" moniker to refer to police officers and their branches within the RCMP. Further, while interviewing an individual responsible for implementing the RCMP's Digital Policing Strategy, I frequently had to interrupt them to ask them to explain what they meant by how their department had embraced "Agile" or "Waterfall" models in spearheading police technology initiatives (these turned out to be business management philosophies originating in the software development industry). Taken together with the discussion in Chapter 3 of how police view transparent communication about technology as "marketing," policing's embrace of managerialist jargon suggests a public sector institution in the throes of an identity crisis. Police are caught between their status as a public sector agency and their growing reliance on private sector technology.

Police's growing reliance on technology consultants also highlights how the private sector's encroachment on Canadian policing does not just appear in the way police administrators

speak about technology. Police have turned toward a handful of private sector models that represent further blurring of public and private in police technology, one of which being the private consultant model of organizational change. A law enforcement administrator with prior experience leading innovation efforts in a Canadian police department explained this increased reliance on private-sector consultants as stemming from the need for "specialized" knowledge and resources for technological transformation in policing. This administrator, in explaining the role of consultants, told me that police are "paying them to stay on the cutting edge," and that they help break beyond "the old traditional models" within policing that can stagnate innovation. The two police technology consultants with which I spoke described their work in similar terms, as outsiders who bring in project management and technological implementation expertise that police would not otherwise have.

Another compelling yet understudied model is the curious emergence of police technology 'incubators' or accelerators, which takes the private sector model of start-up incubators and plops it into the public sector context of policing. There are a handful of these incubators operating within Canada, with the express goal of developing technologies for public safety within a confined regulatory space. One such example is the V13 PoliceTech Accelerator program, run as a cooperation between the Northumberland Community Futures Development Corporation (Northumberland CFDC)—which is funded by Canada's Federal Economic Development Agency for Southern Ontario (FedDev Ontario)—and the Coburg Police Service (CPS) in Southern Ontario. According to someone I spoke with who administers the V13 PoliceTech Accelerator, the Accelerator is designed to help start-ups and small-to-medium enterprises design, test, and validate new technologies, presenting them the opportunity to pilot their tools with the CPS. The program also provides those who work with them a benefit unlike those presented in other police technology contexts. To quote the abovementioned individual from the V13 PoliceTech Accelerator:

> "So our program, we request the right of first deployment. So we will test validate a system and work with them to build out the application or the technology itself. At the end of that project, we reserve the right for a time limited window to be the first purchaser of that technology at a reduced cost in, say, Canada, yeah. And companies love that because they're like, "Wait, you're going to potentially purchase our equipment at the end. That's amazing."

A similar model exists in Edmonton, Alberta. The TELUS Community Safety and Wellness Accelerator is the product of a partnership between Silicon Valley accelerator AlchemistX; the

Edmonton Police Foundation, a charitable organization devoted to "rais[ing] funds to advance excellence and transform community policing in support of the Edmonton Police Service"; and Alberta Innovates, a Canadian crown corporation created and funded by the government of Alberta meant to promote innovation in the province. The combination of funding between private sector entities like AlchemistX and the public sector funding of the province of Alberta make this program a bit of a regulatory mess, but the involvement of the Edmonton Police Service in using the Accelerator's technologies points to further collapse between traditional public- and private-sector boundaries in police technology. These boundaries have already begun eroding by virtue of how police administrators talk about technology, and by virtue of the involvement of consultants in police technology projects, and these boundaries will continue to erode as the incubator and accelerator models expand to equip more Canadian police with more private-sector technologies.

One final way in which a private-sector mentality has suffused the public-sector administration of police technology is in the 'innovative' ways police have come to govern it. Consistent with Skogan (2008) and Weisburd & Braga's (2019) conception of police reforms as synonymous with police innovations, some of the early entrants into the governance of police technology represent innovative approaches to reforming police practices. However, I present a complication: while some, like Toronto police institutions, deliberately construct themselves as innovators and their new governance models as innovative, others like the RCMP explicitly shy away from viewing themselves as innovative, even if their emerging program for governing police technology represents a novel intervention.

In their policy documents, the TPSB and TPS have deliberately leaned into highlighting the bright and shiny newness of their governance documents. As mentioned in Chapter 1, the TPSB highlights the uncertain legal terrain in which they are operating. However, it is worth emphasizing that the TPSB highlights this uncertain legal terrain by positioning themselves as innovators within it who are developing cutting-edge governance without the help of precedent. For example, in the call for public consultation, the TPSB's AI Framework webpage says that "This Policy is being developed in a field with few existing examples and no established guidelines or best practices. To our knowledge, this will be the first Policy of its kind among Canadian Police Boards or Commissions" (TPSB, "Public Consultation," 2021). As a result, the TPSB continues, "The Board is stepping into this new space in recognition of the importance of governing this field, but also

recognizing that a Policy governing AI technology use by the Service will have to itself be innovative" (ibid).

This innovation-centric language made its way into the formal language of the codified TPSB's AI Policy, too. As written, the Policy states that "No current statutes or regulations fully govern the use of AI technologies in Ontario or Canada, and the Province has not yet developed comprehensive guidelines for the use of such technologies in policing," and "as a result of the current legal gaps and desired use of AI technologies, the Board determines it necessary to establish governance to facilitate decision-making that is in the public interest" (TPSB, AI Policy, February 2022). This language further asserts the TPSB's status as innovators who have to make the rules themselves if no one else will.

Even though the TPSB's AI Policy was formally ratified two years ago, the TPSB continues to gesture toward the Policy's innovative status. In a board report from January 11th, 2024 (the first update on the TPSB's policy in almost two years), the TPSB issued a motion to amend its AI Policy. In so doing, the TPSB's motion refers to the AI Policy, once again, as "a first of its kind in the world," still emphasizing the novelty of the governance artifact despite its ratification in 2022. In fairness, this emphasis on novelty is somewhat justified; to date, no other municipal police service in Canada has established a similar policy, or at least no other agency in Canada has done so publicly. With that said, I argue that the TPSB's continued emphasis on the AI Policy's novelty provides the TPSB with a safety net to fall back on should the policy encounter any trouble, and served as a bulwark against criticism as the TPSB attempted to revise the Policy's language. But emphasizing this novelty, I argue, also appears to be the TPSB's way of bolstering their legitimacy as a one-of-a-kind police force at the vanguard of safe technology practices.

Like the TPSB, the TPS emphasizes the novelty of their draft AI Procedure but does so with a subtler approach. For one, the TPS' draft AI Procedure's consultation page can be found under the "Police Reform" tab on the TPS' website, which features a "Police Reform Implementation Dashboard," prepared by the TPS' Analytics & Innovation unit, monitoring the TPS' progress on implementing recommendations for new reforms to old practices (Figure 6). Further, when the TPS' AI Procedure was available online, it bore three hallmarks of novelty: it was watermarked with "DRAFT" on it; it did not have an official issued date, instead bearing a series of X's where a date would otherwise be; and its status was listed as "new" (Figure 7). Before

it was taken offline for unspecified reasons, the TPS' AI Procedure thus presented itself as a bleeding-edge artifact that was so ahead of the curve that it did not even *exist* yet.

What is more, the TPS uses the Procedure to advance an argument for the necessity of technological innovation, framing adopting novel applications of AI as something that either improves expected police services or keeps them consistent. "Technology," goes the Procedure, "can provide opportunities to improve efficiency and customer service, resolve complex issues, ensure business continuity, and provide assistance in performing repetitive tasks." The Procedure frames adopting AI as that which can "provide effective policing," "maximise [the police's] ability to protect the public," and "support the Service's mission to deliver police services, in partnership with our communities, to keep Toronto the best and safest place to be." The TPS must innovate with AI, says the Procedure, so the Service can "*remain current* in its ability to effectively investigate alleged criminal behaviour" (emphasis added). The TPS' AI Procedure thus presents the TPS as innovative in their use of technology, and innovative in their approach to governing it.

Figure 6: TPS' Police Reform Implementation Dashboard, prepared by the TPS' Analytics and Innovation unit.

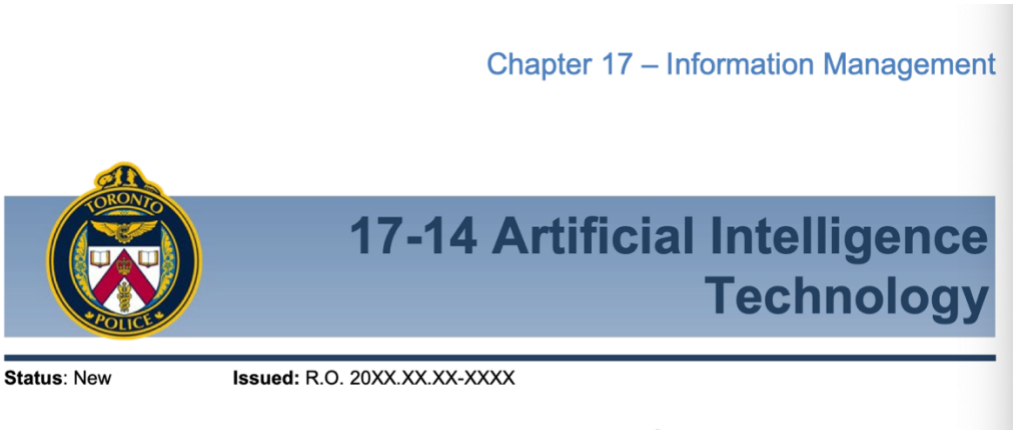


Figure 7: TPS' draft AI Procedure, a novel artifact.

Like TPSB and TPS' AI Policy and Procedure, the RCMP's National Technology Onboarding Program is a first-of-its-kind technology governance model, but unlike Toronto policing institutions, the RCMP actively avoids framing itself or NTOP as innovative. Instead, NTOP highlights itself as built upon a pre-existent governance network, its genesis in RCMP programs and resources predating the establishment of NTOP, and one that brings together components of different branches and units to cover its various commitments in oversight and governance.

Internal documents and discussions with members of the RCMP see NTOP downplayed as an innovation, emphasizing instead its origins in pre-existing features. As discussed in Chapter 1, NTOP was developed to fill the regulatory gaps exposed by Clearview AI by bringing the RCMP's disparate units and branches into lockstep with one another and centralizing the assessment and evaluation of new technology. When asked about how NTOP came to be in its current form, an NTOP representative said it originated not as a new entity, but as "an expansion of what we started with TCMP," referring to the Technical Case Management Program, a program that regulated the use of the RCMP's use of digital surveillance tools. When NTOP originally began, this representative continued, "I think originally it was looked at just as a mailbox: 'Send your thoughts to us, and we'll let you know if you should be using the tool or not.'" Deeming this mailbox model insufficient, this NTOP representative realized that "we have to look at this as a whole-of-government, probably really all-of-law enforcement problem that we need to address.'" The representative noted that the NTOP process grew to become "not about redoing things that already exist. And often, part of the NTOP process is making sure people are aware of existing steps that involve those other players already." Thus, in describing NTOP's iterative development, the

RCMP downplays how progressive the program really is: NTOP, I was told, is not about reinventing a regulatory wheel, but about synthesizing disparate parts and governing technology through existing mechanisms.

Even if NTOP's representatives do not consider the program to be an innovation, I argue that it nevertheless qualifies as an innovative reform, as it involves the recombination and networking of RCMP stakeholders for a novel purpose. NTOP revolves around a network of internal RCMP branches, units, and programs. According to internal documents, NTOP's operations hinge on smooth collaboration between the RCMP's Access to Information and Privacy (ATIP) branch for *Privacy Act* compliance and disclosures about technology; the Legal Services Unit (LSU) to ensure the proposed technology is compliant with the *Charter* "and other applicable laws and regulations"; and close collaboration with the Action, Innovation and Modernization (AIM) office to provide regulatory analysis and correction when "any aspect of the [proposed technological] capability (such as deployment, training, or policies) may create barriers to equity, diversity, or inclusion" (A0764529, pp. 68). It also involves close collaboration with the RCMP's Information Management/Information Technology (IM/IT) program to determine if an NTOP client requires technical advice, risk assessment, or issue management with respect to their proposed technology; the Technical Case Management Program (TCMP), "to provide guidance on how to use, protect, disclose, and monitor capabilities that have been deemed sensitive in nature"; its Departmental Security Information and Communication Technology Security (DS-ICTS) program, to determine if a proposed technology requires a higher-level security assessment and authorization; the RCMP's Professional Ethics Office, "when the capability's evaluation creates any ethical concerns including bias"; as well as "Designated Divisional NTOP Liaisons" meant to provide touchpoints for NTOP to different RCMP divisions across the country (ibid., p. 30, 38, 68).

Thus, NTOP's success, I learned from participants and internal documents, hinges on this "multi-tier governance model" and the "close working relationships" between these units and NTOP management (ibid.). Consistent with the consensus-driven power-sharing arrangements advanced by network and collaborative governance frameworks, here is one of the individuals responsible for NTOP talking about the interconnection of NTOP and other units, speaking to the importance of a collaborative stakeholder network in making sure NTOP governs technology effectively (Hermansson, 2016; Purdy, 2012; Ran & Qi, 2019):

> "So a perfect example is if someone is contemplating a technology that uses or collects personal information, we will ask them in our intake form, does the tool collect personal information? If the answer is yes, our next step is to engage ATIP. So ATIP's work is part of our process. So it's not that there's an ATIP process and an NTOP process: NTOP's outcome is the inputs are 'the proper IM/IT process, the proper ATIP assessment, a thorough Department of Security Branch assessment,' all of that combined equals 'You've successfully gone through the NTOP process."

Despite its status as the first police governance program of its type in the world, NTOP further downplays its innovative structure by openly acknowledging the inspiration it drew from other governance frameworks. The figure below is a screenshot from an undated slide deck about NTOP (Figure 8). In the slide's bottom right corner is a small text box titled "Resources," which points to two resources that were used in the development of NTOP. The first listed resource is the IACP's (of Technology Conference fame) Technology Policy Framework. The Technology Policy Framework was created by the International Association of Chiefs of Police to guide the IACP's constituent members in developing their own policies around technology, and to better ensure that police do not use technologies in a way that could violate civil rights or liberties (IACP, 2014). The RCMP specifically acknowledges that it drew on information from the Framework's mandate, universal principles for good technological governance, as well as the Framework's sample policies—once again situating its origins in pre-existing police technology governance structures.

The second listed resource on the slide below is "NYPD Surveillance Technology," referring to the New York Police Department's (NYPD) Public Oversight of Surveillance Technology (POST) Act. The POST Act municipal legislation meant to increase monitoring and transparency around the NYPD's use of new technology. The slide below cites that NTOP took inspiration from the POST Act's policies requiring the NYPD to evaluate the impact and use of their own technologies, as well as transparency provisions requiring the NYPD to disclose a list in-use surveillance technologies with the public. All of these POST Act components are reflected within NTOP's internal policies, but NTOP does something new with them, using them as the jumping-off point for establishing a program with no other precedent or equivalent on a federal scale.

Thus, despite police technology vendors' suggestions that police departments are not themselves innovative, some Canadian police departments have drifted toward practices that some might regard as more consistent with an historically more innovative private sector. Some police

administrators in charge of technological initiatives have adopted corporate-speak to better fit in with the private sector; some have embraced private technology consultants and incubator models to streamline technological projects. And some have looked to technology governance as an opportunity to be innovative, developing cutting-edge reforms with virtually no Canadian or international precedent. Policing institutions like those in Toronto have used these governance reforms to bolster their own status as vanguard innovators intervening on barren land, reveling in the novelty of their interventions by identifying it as "a first of its kind in the world" (TPSB Meeting, January 11, 2024, p. 2). Others, like the RCMP, have taken whatever opportunity they can to downplay just how innovative their technological governance program really is. Unlike Toronto policing institutions, the RCMP recognizes that the land is not as barren as some might think. NTOP is innovative in that it is unprecedented, but the RCMP situates NTOP within a wider, more collaborative governance network. This network is comprised not only of internal units working together; it is comprised of the influence and information of external actors, like the IACP, and of external artifacts, like the POST Act. Pointing to pre-existing governance actors and documents grounds NTOP in stable governance space, masking over NTOP's innovativeness by emphasizing the familiar.

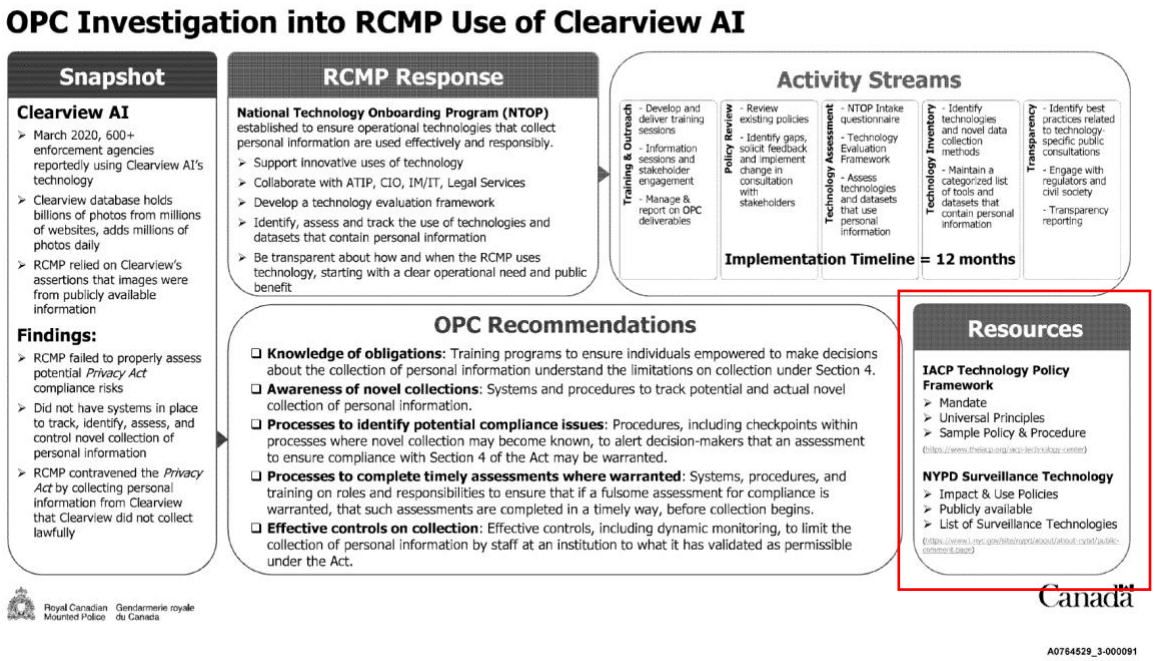

OPC Investigation into RCMP Use of Clearview AI
Snapshot
Clearview AI
March 2020, 600+ enforcement agencies reportedly using Clearview AI's technology
Clearview database holds billions of photos from millions of websites, adds millions of photos daily
RCMP relied on Clearview's assertions that images were from publicly available information
Findings:
RCMP failed to properly assess potential Privacy Act compliance risks
Did not have systems in place to track, identify, assess, and control novel collection of personal information
RCMP contravened the Privacy Act by collecting personal information from Clearview that Clearview did not collect lawfully
RCMP Response
National Technology Onboarding Program (NTOP) established to ensure operational technologies that collect personal information are used effectively and responsibly.
Support innovative uses of technology
Collaborate with ATIP, CIO, IM/IT, Legal Services
Develop a technology evaluation framework
Identify, assess and track the use of technologies and datasets that contain personal information
Be transparent about how and when the RCMP uses technology, starting with a clear operational need and public benefit
Activity Streams
Training & Outreach
- Develop and deliver training sessions
- Information sessions and stakeholder engagement
- Manage & report on OPC deliverables
Policy Review
- Review existing policies
- Identify gaps, solicit feedback and implement change in consultation with stakeholders
Technology Assessment
- NTOP Intake questionnaire
- Technology Evaluation Framework
- Assess technologies and datasets that use personal information
Technology Inventory
- Identify technologies and novel data collection methods
- Maintain a categorized list of tools and datasets that contain personal information
Transparency
- Identify best practices related to technology-specific public consultations
- Engage with regulators and civil society
- Transparency reporting
Implementation Timeline = 12 months
OPC Recommendations
Knowledge of obligations: Training programs to ensure individuals empowered to make decisions about the collection of personal information understand the limitations on collection under Section 4.
Awareness of novel collections: Systems and procedures to track potential and actual novel collection of personal information.
Processes to identify potential compliance issues: Procedures, including checkpoints within processes where novel collection may become known, to alert decision-makers that an assessment to ensure compliance with Section 4 of the Act may be warranted.
Processes to complete timely assessments where warranted: Systems, procedures, and training on roles and responsibilities to ensure that if a fulsome assessment for compliance is warranted, that such assessments are completed in a timely way, before collection begins.
Effective controls on collection: Effective controls, including dynamic monitoring, to limit the collection of personal information by staff at an institution to what it has validated as permissible under the Act.
Resources
IACP Technology Policy Framework
Mandate
Universal Principles
Sample Policy & Procedure
NYPD Surveillance Technology
Impact & Use Policies
Publicly available
List of Surveillance Technologies
Royal Canadian Mounted Police / Gendarmerie royale du Canada
Canada
A0764529_3-000091

Figure 8: NTOP slide featuring resources that informed its development.

Conclusion

Among police institutions, technological innovation is often conceived as an alluring silver-bullet solution to a host of problems, from preventing crime to detecting it, from streamlining resource management to holding officers accountable for misconduct (Ariel, 2019; Ferguson, 2017; Koper & Lum, 2019). Technological innovations, when they work, are believed to make police more professional, more objective, and fairer (Capers, 2017; Chan, 2001; Joh, 2016; Leman-Langlois, 2011; Sanders, Weston, & Schott, 2015). But say 'regulation' in the same paragraph as 'innovation' and observe as rhetoric shifts among the more business-minded that regulation "will stifle innovation and progress," bringing to mind the concern that current laws and regulations are insufficient to deal with the complexities that new technologies create for them (Dignum, 2020, p. 224).

This chapter established that when it comes to police technology, the relationship between technological change and regulation is far more complicated. Of course, as shown by the technology vendor who provided a guided tour of the police technology sales process, the sale of police technology often requires the careful balance of multiple stakeholders and the consideration of the unique social and political circumstances of the police department buying the technology. But as soon as one strays from the conventional sales path, technological innovation in policing unfolds against a contested and uncertain regulatory backdrop, one which either helps or hinders its progress. To some within policing, and those operating in the tech sector as vendors, it is either the lack of governance or governance's bad fit for vendors that stifles police innovation, either causing police and tech vendors to go about innovation without proper processes or causing them to hold off on technological innovation altogether. What is more, overabundant regulation is said to drag technological innovation down to a crawl, with strict procurement rules and multi-layered decision-making precluding technological innovations from unfolding altogether. But to those within civil society, overabundant regulation might be the sole bulwark between harmful technologies and the greater concentration of police power.

Further, the slippery boundaries between public and private that emerge when police use technology breed frictions between police technology stakeholders and within police departments themselves. On top of private vendors chafing against the restrictive nature of public sector governance, some police find their technological identities in crisis, leaning toward an increasingly corporatized way of speaking about technology projects and a greater reliance on private sector

innovation models. To that end, some police departments have responded to the technological changes in policing with regulatory changes of their own. In their struggle to be being pure technological innovators, police have started innovating in how police technology is governed, further suggesting that policing innovations are possible even if innovation does not mean a shiny new toy in their toolbelt.

Though technological change in policing is unfolding in fits and starts, the *appeal* of technological change is ever present. As police's use of AI-enabled tools grows, and as these technologies create new problems for police and publics alike, Canada will need to respond to police innovation with innovative governance solutions.

Conclusion: Governing the (Automated) Thin Blue Line

Shortly before the last set of panels is set to begin, I bump into a retired police administrator with whom I had fallen out of touch some months prior while trying to arrange an interview. They are profusely apologetic, and we settle on opposing sofas across from an elevator bank so we can finally chat. Our conversation unfurls in zigs and zags; this individual is a philosopher in a police reformer's body, and I struggle to follow their tangents, which take us everywhere from partisan politics to Pac-Man machines. Finally, I hit the good cop with a bad cop routine and steer our conversation into more relevant waters. My participant waxes poetic about how a lack of public trust in police technology is at once a lack of trust in both policing and technology. They dip into business-heavy jargon: building public trust in police technology is about "finding the value-added proposition," and police can use AI to deliver "customers" a "predictable product" of safety. We spar about the necessity of knowledge to police technology debates, and how "the most important component" of getting the public to trust police technology is getting them "to understand" it. They preach about stakeholder politics, asking me how police should be expected to "sell" technology to groups that do not want to receive it, and how hard it is to find "the delicate balance of the political appetite of the community" when it comes to using technologies that bring safety at the expense of civil liberties. Then, my interlocutor veers back toward the allegorical and the arcane. "Governing police technology," they tell me, "is like putting an artificial piece of saran wrap on a glass that continues to grow." I am not exactly sure what that means, but before I can clarify, they are standing up and wishing me well on my project. "I really admire you taking this on," they tell me, reaching out to shake my hand. "Because it's a dicey subject."

Sitting at the nexus of two hotly contested phenomena, police technology has emerged as a controversial subject, not only because of declining trust in policing, or increasing concerns about technology's power, but because of challenges with police technology governance. Whether at the municipal, provincial, or federal level, Canada has struggled to adequately regulate police technology. The fallout of the Clearview AI controversy, in which police across the country at all three levels of service used privacy invasive FRT without disclosing its acquisition to the public, led to the creation of governance mechanisms to compensate for previously unregulated use has shone light on the many ways in which governance in the police technology is an empty promise. As we have seen throughout this project, though, existing governance frameworks for either police or technology frequently struggle to regulate the combination of both. Too often do architectures

of secrecy preclude those outside of policing from knowing about police technology, stymieing any possibility of transparency and thus accountability of these tools—information about these tools is something that stakeholders like journalists have to *dig* for, and is not something that is voluntarily given (and even when it is given, it is often redacted or heavily edited in FOI releases, so the picture we get of police technology is never complete). Even attempts to innovate within technology create disadvantage, as the regulatory structures in place to prevent abuse might be too onerous for technology vendors to actually follow, or not onerous enough to effectively regulate powerful technology. And many stakeholders wrapped up in discussions of police technology are off kilter from one another, with regulatory power clustered among those with the greatest interest in flouting it. This often means that consultations with members of the public about police technology are left entirely at the discretion of police administrators, while attempts at regulation by governmental bodies with no order-making power, like privacy commissioners, are free to be ignored.

Overall, this project demonstrates the complexities inherent to the governance of police technology. It shows that studies of police technology cannot just focus on the technology itself or police institutions alone: they must explore the heterogenous stakeholders who orbit its use and affect its regulation. It demonstrates the importance of thinking wide about those actors and institutions, as doing so allows for more complete understandings of those who stand to influence the ways police technology is governed—or whose influence may be denied. As we have seen, the network of actors and institutions within police technology is vast. There are police departments, themselves comprised of many units and actors, oftentimes in tension with one another about the oversight of the technology in their own arsenal. There are governing bodies like police boards, who set and enforce technological policies, and there are governmental bodies with mandates to govern police or technology but rarely both at once. There are arms-length regulators, like privacy commissioners, who oversee compliance with law but who do not have the power to enforce it. There are non-governmental organizations, like advocacy and academic groups, who advocate for technological reform but find their consultative influence limited by police. Then there are private sector actors like police technology vendors and consultants, who sell their tools to police but occasionally find themselves struggling to do so given police's conflicting attitudes toward innovation and regulation. There are journalists, who surface otherwise hidden information about

the tools technology vendors provide police, and they convey this information largely to the public, who are frequently left out of shaping the governance of police technology.

This project highlights the importance of using controversy as an analytical vantage point that widens the scope of who is involved in questions of police technology governance. Explorations of police technology are not just about the technology itself: they are about the actors and institutions with a stake in how these technologies are used and regulated; the politics of knowledge that keep technology secret and keep stakeholders in conflict with one another; the tensions that complicate interactions between public service and private enterprise; and the challenges of creating meaningful technology governance in ambiguous legal space. To call back to a quote from a police technology consultant in Ontario, "Clearview was a whole different shenanigan."

What an understatement.

Implications and Directions for Future Research

How do governance structures limiting the use of police technologies take shape in Canada? Who are the different groups involved in building these guardrails, with what knowledge and toward what ends? How do the tensions between these groups resolve themselves in the creation of various types of regulatory mechanisms? And what of the configurations and consequences of these mechanisms themselves? All of these, and more, are questions which I attempted to answer, at least in part, throughout this project, but are questions that would benefit from greater scrutiny in other jurisdictions, with other police forces, and with other forms of technology.

a. Expanded Case Studies and Refinement of Controversy's Source

Scholars looking to expand this area of research should look to more case studies of police use of technology, and angle to unpack why certain technological projects invoke controversy and others do not. Controversy, in its most traditional sense, is endemic to policing writ large. Policing is a naturally controversial undertaking, what with the practice's long history of—and occasional public reckoning with—police brutality, racial and socioeconomic discrimination, and financial corruption. These are well-documented in policing scholarship. However, technological controversies in policing are *not*, despite it being something with which police—the TPS, the OPP, and the RCMP included—are intimately acquainted.

However, police use of technology is not inherently controversy prone, and police do not always go about technological acquisition in secret. The TPS' proposed acquisition of ShotSpotter failed to materialize after the privacy-invasive surveillance technology courted controversy from Toronto City Council and civil advocacy groups (Gillils, 2018; Janus, 2019). IMSI catchers, or Stingrays, were the source of scandal when their use was kept hidden from the public (Seglins, Braga, & Cullen, 2017). But as shown by the TPS' BWC pilot project (TPS Strategy Management, 2016) and the RCMP's test-run of automated license plate readers (ALPR) in Surrey, British Columbia (Denham, 2012), police in Canada have shown that they are capable of going through relatively legitimate and relatively open steps to acquire, govern, and use cutting-edge technology. More case studies of police technology acquisition and further study are needed to better understand the conditions in which police use of technology is and is not considered controversial.

b. Comparative Research on Hard Law

Future research should adopt a comparative approach to the hard law governance of police technology. Canada is but one jurisdiction in technologically advancing world, and researchers may find compelling examples of technology governance beyond our borders—examples which may help inform how Canadian laws are developed. One worthwhile point of comparison is in hard law around AI. Canada's omnibus Bill C-27, the *Digital Charter Implementation Act*, features the *Artificial Intelligence & Data Act* (AIDA), is poised to be Canada's first piece of legislation governing the emerging threats around AI. But as it stands, there is no legislation specifically devoted to the police's use of technology in Canada.[37] Bill C-27 would make for an interesting point of comparison against the European Union's AI Act, whose recent ratification shows that it is possible to create hard law regulating technology used in the course of law enforcement.

Further research may also look to municipal and state models for governing police technology emerging in the United States. One such example is, as mentioned earlier, New York City Council's enactment of the Public Oversight of Surveillance Technology (POST) Act. The bill requires the New York Police Department (NYPD) to disclose information about the surveillance tools in its utility belt. Specifically, the Act requires the NYPD to produce and publish

[37] AIDA contains a carveout exempting itself from application to law enforcement in Canada, meaning the bill fails to capture privately developed AI systems used in the course of policing. Bill C-27 also contains no formalized safeguards to prevent against the non-consensual collection of biometric information, which can create the conditions for FRT systems to harvest images of people's faces without their consent.

Impact and Use Policies (IUPs) for each surveillance tool. According to an assessment of the NYPD's response to the POST Act conducted by the NYPD's Department of Investigation's Office of the Inspector General for the NYPD, the model has had mixed success, as the NYPD has failed to comply with some of the POST Act's transparency and disclosure requirements (McDonough, April 13, 2023; NYC Department of Investigation, 2022; NYPP, December 15, 2023). However, future research should examine the success and failures of the POST Act to understand the viability of such a model for Canadian contexts.

c. Theorizing and Testing Best Practices for Improved Stakeholder Engagement

Future research should focus on establishing and testing best practices for stakeholder engagement in a regulatory space as contested and ambiguous as that surrounding police technology. Standards of good governance often include deepening stakeholder participation, but research is still needed on how this can be bolstered in police technology. One promising area of study to this effect is the emerging scholarship on 'democratizing AI' (Gilman, 2023; Wilson, 2022). Scholars writing on democratizing AI have highlighted ways to improve public participation in the development of AI governance. Methods for improving participation include institutionally budgeting for public consultations, conveying consultations in clear and accessible language, and providing clarity on which aspects of policy can be influenced by consultation and which ones cannot (Ada Lovelace Institute, 2023; Corbett, Denton & Erete, 2023; Gilman, 2023; Wilson, 2022; Wong, 2023).

While principles for democratized AI governance have been evaluated in a number of contexts, the context of AI in policing is not one of them. In Canada, few have had the opportunity to empirically evaluate the experiences of the public in the police technology context. What is more, discussions of democratizing AI focus primarily on including the public in stakeholder consultations, when there are so many other actors and institutions—in government, civil society, and journalism—who would benefit from improved stakeholder relations with police. Future research on democratizing AI in policing could help establish a set of recommendations for police departments to improve their approach to consultations and could serve as the basis for improved collaboration on matters as controversial as the acquisition and governance of technology.

d. Public Surveys on Correlations between Trust, Legitimacy, and Knowledge

Data from outside of Canada validate a correlation between knowledge of technology and trust in institutions. A comparative study of public attitudes towards FRT in China, Germany, the UK, and the United States found that people who had greater trust in government institutions were generally more willing to accept FRT in public spheres, and that people's awareness and knowledge of a country's prior history with surveillance shapes their perceptions and acceptance or rejection of FRT (Kostka, Steinacker & Meckel, 2023). Another study found that "different reporting in the media" can shape public opinions about FRT in different countries, but that for the most part, "the capabilities of FRT seem to be decoupled from both public understandings and extant policy," suggesting a public generally unaware to FRT's presence and applications in a given nation (Ritchie et al., 2021, p. 5). And a study conducted on public attitudes about FRT in the UK found that though 90% of respondents said they were aware of the use of FRT, only 53% said they "know something about it"; support for the use of FRT was contingent upon levels of trust in the institutions using it; and most respondents were confused about FRT, believing it to be more accurate than it actually is (Ada Lovelace Institute, 2019).

This mess of findings points to a tricky but important connection between how much people know and understand police technology and how much people trust police and deem them legitimate—one that is yet to be teased out in a Canadian context. Further research can build upon these international findings by adopting similar surveys as the ones conducted above and applying them in a Canadian context.

e. *The Viability of Alternate Modes of AI Governance*

Future research should explore alternate modes of governing police technology. Amid today's AI boom, scholars working at the intersection of computer science and public administration have proposed novel modes of governing AI that require further study to assess their viability for policing contexts. Further, while some of these alternate modes of governance present promising solutions to governance problems, they too open up further stakeholder networks to explore and unpack.

Some of these scholars have proposed designating any AI systems that pose severe risks to public safety as "frontier" models meriting additional safeguards, and subjecting these tools to more rigorous risk assessments as well as regulation from government to ensure institutions

outside of industry are monitoring private sector compliance (Anderljung et al., 2023; Shevlane et al., 2023). Other scholars have proposed algorithmic auditing, which prioritizes independent assessment of AI systems against clearly defined safety standards, as well as an emphasis on evaluating real-world harms created by the AI system under review (Costanza-Chock et al., 2023; Vecchione, Levy & Barocas, 2021). Others have proposed the adoption of certification systems for certifying AI systems as in alignment with certain technical and ethical criteria (Cihon et al., 2021; Henriksen, Enni, & Bechmann, 2021). Scholars from New York University's Policing Project have already proposed an application of this approach in the context of police technology: in the absence of meaningful "hard law" on police technology, Barry Friedman, Farhang Heydari, Max Isaacs, and Katie Kinsey (2022) propose the creation of a "soft law" certification scheme, whereby an independent body would be tasked with performing an "efficacy review and an ethical evaluation" of technologies, evaluating the implications of police technologies for privacy, racial justice, civil rights and liberties.

As police may find themselves using more and more AI in their pursuit of greater efficiencies, future research should evaluate whether current means of governing police use of AI provide adequate regulation, and whether emerging modes of AI governance can offer helpful solutions to the current governance regime's problems.

Questioning the Algorithmic Present, Governing the Algorithmic Future

Effective and meaningful technological regulation is so challenging because governance is often positioned as a panacea to solve all woes, but much of the problems that plague police technology are more systemic and existential. We covered the asymmetrical power relations that bely seemingly more horizontal arrangements of regulation, the private interests that create unequal outcomes in procurement processes, the architecture of secrecy that precludes publics from knowing about the police's use of technology, the police's self-professed problems with "marketing" themselves and their technological arsenal, and the disjunct that arises between police's desire to innovate and what regulations actually allow—all of which point to a fundamental brokenness of governance mechanisms, or which cause those mechanisms to backfire. To wind our way out of this digital quagmire, the governance of police technology in Canada needs to be fundamentally reimagined, creatively so, and fast. Otherwise, police may run the risk of cultivating a reputation as irresponsible technological actors, all while powerful

technologies with dire implications for civil rights churn on with spotty checks and spottier balances.

Having strong policies governing the deployment and use of police technology is essential to effectively sustaining technological implementation and is essential to maintaining community trust in technology (IACP Technology Policy Framework, 2014). But right now, there are too many gaps within existing governance processes to ensure that police technology is used and monitored thoughtfully. Attempts at governing this space are noble and necessary, of course, but as the examples in this project have highlighted, these governance attempts false promises. To get police back to transparent, trustworthy, and thoughtful engagement with technological innovation, we need radical solutions for radical results.

Until then, police technology will continue to be a source of controversy. Of course, controversy is an important analytical tool: it reveals stakeholders bound up in questions of police technology, it teases out their connections and underlines their differences in red, and it helps clarify how different groups make sense of technology. Controversy is also sunshine-as-disinfectant. Every now and then, the public comes to learn about police technologies long after the technologies have been in use, usually because of dogged journalists, as was the case with the TPS' and RCMP's use of both Clearview AI's facial recognition system. Academics, civil society, and even governmental agencies are largely left to speculate on these basic questions about police technology, creating power imbalances within the stakeholder network that surrounds the governance of police technology.

Controversy also serves, as in these three cases, as the impetus for finally trying to get ungoverned space under control. The Clearview AI controversy inspired Canadian MPs to call upon privacy commissioners to investigate the company, which inspired privacy commissioners in Quebec, Alberta, and BC, in tandem with the federal OPC, to launch a joint investigation into Clearview AI, which resulted in the creation of a joint statement calling on legislators to change laws and a guidance document to clarify regulations around FR. It inspired the RCMP to create NTOP, and it inspired the TPSB to create an AI Framework. These governance reforms and innovations are by no means perfect, and their attempts at governance are hampered with faults from within and faults from without. More research—more *interdisciplinary* research that blends sociolegal studies and criminology and policing studies with STS—is needed to monitor the aftereffects of these mechanisms, and to see how they play out, but early signs point to a need for

further reform. Ideally, police departments will be more willing participants in conversations around how to improve these nascent policies, and ideally, police will bring all the stakeholders in the web encircling technology to the table.

But many stakeholders described good governance in much the same way: that tools are being monitored, of course, but first and foremost, that there is transparency in how they are acquired, in how they are used, and how they are controlled. As one proud civil society advocate told me when I asked them what good governance of police technology would look like, they told me: “We have to know what technology they’re using. That would be the first thing.”

Postscript: Packing Up the Black Box

The conference is winding down. I stop by the exhibit hall after my chat wraps up with the philosopher-come-reformer, only to find vendors packing away their booths. Roaming around the detritus of three days of trade show madness, I stumble upon a sales rep from Panasonic, who tells me they got a head start on teardown because their team is off to host a casino night at a nearby bar. They give me their card (again—I had met him the day before) and encourage me to reach out if I want to interview them for my project. When I tell them how grateful I am for their generosity and how shocked I am by their openness, they slap me on the shoulder and say, "I have a son who just finished college, so I'm empathetic to your whole thing."

As I walk out of the disassembled exhibit hall, I reach into my tote bag to take stock of all my company-branded swag. There are socks from a company called Flock, which has branded itself the "ethical police technology company." Here are all the pamphlets about quick and easily integrated solutions for the toughest policing problems. And here is a strange, bright blue Clearview AI-branded bendy stick, which is all I got for stopping by their booth.

My flight leaves later that night. I head back to my room, grab my bags, and make for the exit. As I'm stepping onto the first step at the bottom of the escalator's, there's a person just getting off at its top.

He presses the button beneath the "Push button to play polka" sign.

A *wall* of polka music blares from speakers running all along the side of the escalator. What a send-off.

As I crest the top of the escalator, the button-pushing perp is nowhere in sight. I see a convention centre staff member, who is patiently standing before a table, greeting people as they come and go. She is oddly calm for someone whose job, it seems, is to stand dangerously close to polka music all day.

"Does it drive you crazy?" I ask.

She smiles. "What do you mean?"

"When people push the button," I clarify. "Doesn't it just drive you crazy?"

Her smile disappears as she thinks about it for a moment. It creeps back when she answers.

"I don't mind. I can't do anything to stop them. Some people just have no control."

References

A0764529 (October 2022). RCMP FOI disclosure. 450 pages.

Abbott, A. (1988). *The system of professions: An essay on the division of expert labor*. University of Chicago press.

Abrahamson, D. E., & Goodman-Delahunty, J. (2014). Impediments to information and knowledge sharing within policing: A study of three Canadian policing organizations. *Sage open*, *4*(1), 2158244013519363.

Accountable Tech, AI Now Institute & EPIC. (2023, August 10). Zero trust AI governance. *AI Now*. https://ainowinstitute.org/publication/zero-trust-ai-governance

ACLU. (2022, May 9). Big win, settlement ensures clearview AI complies with groundbreaking Illinois biometric privacy law. *ACLU*. https://www.aclu.org/press-releases/big-win-settlement-ensures-clearview-ai-complies-with-groundbreaking-illinois#:~:text=The%20lawsuit%20alleged%20that%20Clearview,without%20their%20knowledge%20and%20permission.

Ada Lovelace Institute. (2019). Beyond Face Value: Public Attitudes to Facial Recognition Techno https://www.adalovelaceinstitute.org/report/beyond-face-value-public-attitudes-to-facial-recognitio

Aditya, B. I., & Kusumastuti, R. (2023). Collaborative governance in police: A review of research, managerial implication and agenda for future research. *Journal La Sociale*, *4*(5), 250-264.

Aghion, P., Bergeaud, A., & Van Reenen, J. (2023). The impact of regulation on innovation. *American Economic Review*, *113*(11), 2894-2936.

Agranoff, R., & McGuire, M. (2001). Big questions in public network management research. *Journal of Public Administration Research and Theory* 11 (3): 295–326.

Aguilar, B. (2020, February 14). Toronto police chief unaware officers have been using controversial facial recognition software for months. *Toronto Star*. https://toronto.ctvnews.ca/toronto-police-chief-unaware-officers-have-been-using-controversial-facial-recognition-software-for-months-1.4811434?cache=yesclipId104062%3FautoPlay%3Dtrue%3FautoPlay%3Dtrue%3FclipId%3D104069

AI Now Institute. (2023, August 10). *Algorithmic accountability policy: Zero trust AI governance.* https://ainowinstitute.org/publication/zero-trust-ai-governance

Alberta Innovates. (2017, March 21). *Mandate and roles document.*

https://albertainnovates.ca/wp-content/uploads/2023/06/Alberta-Innovates_roles-and-mandate_march_2017.pdf

Allan, G. (2003). A critique of using grounded theory as a research method. *Electronic journal of business research methods*, *2*(1), 1-10.

Altschuler, A. A., & Behn, R. D. (eds.) (1997). Innovation in American government: Challenges, opportunities, and dilemmas. Washington, DC: Brookings Institution Press.

Anderljung, M., Barnhart, J., Leung, J., Korinek, A., O'Keefe, C., Whittlestone, J., ... & Wolf, K. (2023). Frontier AI regulation: Managing emerging risks to public safety. *arXiv preprint arXiv:2307.03718*.

Andrey, S., Masoodi, J., Kwok, T., & Côté, A. (2023). An agenda for responsible technology policy in Canada. *Canadian Public Administration*, *66*(3), 439-446.

Angus, C. (2020, January 27). Re: Possible use of facial recognition technology. *Letter to OPC.* https://69490847-1bbc-4d85-bb17-dc869f025e9a.filesusr.com/ugd/3c9b44_422210f300294964ab7a00a6398058a9.pdf

Ansell, C., & Gash, A. (2007). Collaborative governance in theory and practice. *Journal of Public Administration Research and Theory*, *18*, 543–571.

Ansell, C., and A. Gash. (2008). Collaborative governance in theory and practice. *Journal of Public Administration Research and Theory* 18 (4): 543–571.

Ansell, C., & Torfing, J. (Eds.). (2022). *Handbook on theories of governance*. Edward Elgar Publishing.

Ariel, B., Sutherland, A., Henstock, D., Young, J., Drover, P., Sykes, J., ... & Henderson, R. (2017). "Contagious accountability" a global multisite randomized controlled trial on the effect of police body-worn cameras on citizens' complaints against the police. *Criminal justice and behavior*, *44*(2), 293-316.

Aspray, W., & Doty, P. (2023). Does technology really outpace policy, and does it matter? A primer for technical experts and others. *Journal of the Association for Information Science and Technology*.

Ayling, J., Grabosky, P. N., & Shearing, C. D. (2009). *Lengthening the arm of the law : enhancing police resources in the twenty-first century*. Cambridge University Press.

Bacchini, F., & Lorusso, L. (2019). Race, again: how face recognition technology reinforces racial discrimination. *Journal of information, communication and ethics in society*, *17*(3), 321-335.

Bakke, E. (2018). Predictive policing: the argument for public transparency. *NYU Ann. Surv. Am. L.*, *74*, 131.

Ballestero, A. (2012). Transparency in triads. *Political and Legal Anthropology Review (PoLAR)***35**(2), 160-6.

Barry, A. (2001). Political machines: Governing a technological society. London: Athlone Press.

Barton, A., & Davis, H. (Eds.). (2018). *Ignorance, power and harm: Agnotology and the criminological imagination*. Springer.

Bauhr, M., Czibik, Á., de Fine Licht, J., & Fazekas, M. (2020). Lights on the shadows of public procurement: Transparency as an antidote to corruption. *Governance*, *33*(3), 495-523.

Bayley, D. H. (2006). *Changing the guard: Developing democratic police abroad.* Oxford University Press.

Bedford, S. (2023, September 20). CCTV coming to Prescott. *Recorder*. https://www.recorder.ca/news/cctv-coming-to-prescott

Beer, D. (2019). The social power of algorithms. In *The Social Power of Algorithms* (pp. 1-13). Routledge.

Berkeley, G. E. (1969). *The democratic policeman*. Beacon Press.

Bernstein, A., & Mertz, E. (2011). Bureaucracy: Ethnography of the state in everyday life. *PoLAR*, *34*, 6.

Bevir, M. (2012). *Governance: A very short introduction*. OUP Oxford.

Blair, B. (2019). Royal Canadian mounted police 2018-2019 departmental results report. *RCMP*. https://www.rcmp-grc.gc.ca/en/2018-2019-departmental-results-report/full-report

Blind, K. (2016). The impact of regulation on innovation. *Handbook of innovation policy impact*, *450*.

Bloch-Wehba, H. (2019). Access to algorithms. *Fordham L. Rev.*, *88*, 1265.

Bloch-Wehba, H. (2021). Visible policing: technology, transparency, and democratic control. *Cal. L. Rev.*, *109*, 917.

Bonner, M. D. (2020). What democratic policing is… and is not. *Policing & Society*, *30*(9),1044–1060. https://doi.org/10.1080/10439463.2019.1649405

Borrás, S., & Edler, J. (Eds.). (2014). *The governance of socio-technical systems: explaining change*. Edward Elgar Publishing.

Bradford, B., Yesberg, J. A., Jackson, J., & Dawson, P. (2020). Live facial recognition: Trust and legitimacy as predictors of public support for police use of new technology. *The British Journal of Criminology*, *60*(6), 1502-1522.

Bragias, A., Hine, K., & Fleet, R. (2021). 'Only in our best interest, right?' Public perceptions of police use of facial recognition technology. *Police Practice and Research, 22*(6), 1637-1654.

Breen, K. (2020, March 1). OPP confirms past use of controversial Clearview AI technology. *Global News*. https://globalnews.ca/news/6616892/opp-clearview-ai-technology/

Brennan Center for Justice. (n.d.) The public oversight of surveillance technology (POST) act: A resource page.*Brennan Center for Justice*. https://www.brennancenter.org/our-work/research-reports/public-oversight-surveillance-technology-post-act-resource-page

Brewer, R. (2014). *Policing the waterfront: Networks, partnerships, and the governance of port security*. OUP Oxford.

Brockbank, N. (2021, December 23). Toronto police used clearview AI facial recognition software in 84 investigations. *CBC*. https://www.cbc.ca/news/canada/toronto/toronto-police-report-clearview-ai-1.6295295

Brodeur, J.P. (1983). High policing and low policing. Remarks about the policing of political activities. *Social Problems, 30*(5), 507-520.

Brodeur, J. P., & Dupont, B. (2006). Knowledge workers or "knowledge" workers?. *Policing & society*, *16*(1), 7-26.

Brucato, B. (2015). Policing made visible: Mobile technologies and the importance of point of view. *Surveillance & Society*, *13*(3/4), 455-473.

Brunk, C. G. (2006). Public knowledge, public trust: understanding the 'knowledge deficit'. *Public Health Genomics*, *9*(3), 178-183.

Bryson, J. M., Crosby, B. C., & Stone, M. M. (2015). Designing and implementing cross-sector collaborations: Needed and challenging. *Public Administration Review, 75(5), 647-663.*

Bureaucracy: Ethnography of the State in Everyday Life. PoLAR: Political and Legal Anthropology Review, 34: 6-10. https://doi.org/10.1111/j.1555-2934.2011.01135.x

Burke, D. (2020, February 10). Use of facial recognition technology by police growing in Canada, as privacy laws lag. *CBC*. https://www.cbc.ca/news/canada/nova-scotia/facial-recognition-police-privacy-laws-1.5452749

Burkhalter, E.A. (1998). *The evolution and development of police technology: A technical report prepared for The National Committee on Criminal Justice Technology*. Washington, D.C.: SEASKATE, INC.

Toronto Police Service. (n.d.). *Business with Toronto Police.* https://www.tps.ca/services/do-business-service/

Callon, M., Lascoumes, P., & Barthe, Y. (2009). In G. Burchell (Ed.). Acting in an uncertain world: An essay on technical democracyCambridge: MIT Press Trans

Canada Buys. (2023, December 13). Public procurement. *Government of Canada*. https://canadabuys.canada.ca/en/how-procurement-works/policies-and-guidelines/supply-manual/chapter-1#_1-20

Canada Council for the Arts. (n.d.). Access to information act and privacy acts. *Canada Council.* https://canadacouncil.ca/about/public-accountability/access-to-information-and-privacy-acts

Canada Evidence Act, RSC 1985, c C-5, <https://canlii.ca/t/56471> retrieved on 2024-01-27.

Carboni, J. L., Siddiki, S., Koski, C., & Sadiq, A. A. (2017, September). Using network analysis to identify key actors in collaborative governance processes. In *Nonprofit Policy Forum* 8(2), 133-145.

Carlsson, L., & Sandström, A. (2008). Network governance of the commons. *International Journal of the Commons*, *2*(1), 33-54.

Carney, B. (2020, April 16). *FOI documents confirm RCMP falsely denied using facial recognition software.* The Tyee. https://thetyee.ca/News/2020/04/16/RCMP-FOI-Facial-Recognition/

CBC News. *Toronto police admit using secretive facial recognition technology Clearview AI.* (2020, February 15). https://www.cbc.ca/news/canada/toronto/toronto-police-clearview-ai-1.5462785

Cecco, L. (2022, July 7). 'Asleep at the wheel': Canada police's spyware admission raises alarm. *The Guardian*. https://www.theguardian.com/world/2022/jul/07/canada-police-spyware-admission-surveillance-experts

Chan, J. (1996). Changing police culture. *The British Journal of Criminology, 36*(1), 109-134.

Chan, J. (2001). The technological game: How information technology is transforming police practice. *Criminal Justice, 1*(2), 139-159.

Chanin, J., & Courts, J. (2017). Examining the determinants of police department online transparency. *Criminology, Crim. Just. L & Soc'y*, *18*, 52.

Chanin, J., & Espinosa, S. (2016). Examining the determinants of police department transparency: The view of police executives. *Criminal Justice Policy Review*, *27*(5), 498-519.

Cheng, Y. (2019). Exploring the role of nonprofits in public service provision: Moving from co-production to co-governance." *Public Administration Review* 79(2), 203–214.

Cheng, T. (2023). *The Policing Machine: Enforcement, Endorsements, and the Illusion of Public Input*. University of Chicago Press.

Chermak, S., & Weiss, A. (2005). Maintaining legitimacy using external communication strategies: An analysis of police-media relations. *Journal of criminal justice*, *33*(5), 501-512.

Chin, G. J., & Wells, S. C. (1997). The blue wall of silence as evidence of bias and motive to lie: A new approach to police perjury. *U. Pitt. L. Rev.*, *59*, 233.

CHRC. (2022, April 15). *Facial recognition technology use in Policing*. ttps://www.chrc-ccdp.gc.ca/en/about-human-rights/publications/facial-recognition-technology-use-policing

Christin, A. (2020). The ethnographer and the algorithm: beyond the black box. *Theory and Society*, *49*(5-6), 897-918.

Cihon, P., Kleinaltenkamp, M. J., Schuett, J., & Baum, S. D. (2021). AI certification: Advancing ethical practice by reducing information asymmetries. *IEEE Transactions on Technology and Society*, *2*(4), 200-209.

Cino, J. G. (2017). Tackling technical debt: managing advances in DNA technology that outpace the evolution of law. *Am. Crim. L. Rev.*, *54*, 373.

City of Toronto. (n.d.). *2023 city of Toronto budget summary.* https://www.toronto.ca/wp-content/uploads/2023/05/95f8-2023-City-of-Toronto-Budget-Summary.pdf

City of Toronto. (n.d.). *City of Toronto report 7c.* https://www.toronto.ca/legdocs/mmis/2023/bu/bgrd/backgroundfile-230596.pdf

City of Toronto. (n.d.). *2023 program summary technology services division.* https://www.toronto.ca/wp-content/uploads/2023/04/8e46-2023-Public-Book-TSD-V1.pdf

Cleveland, H. (1972). The future executive. *Public administration review*, *32*(3), 247-251.

Cole, S. (2001). *Suspect Identities*. Cambridge, MA. Harvard University Press.

Colton, K. (1972). Use of computers by police: Patterns of success and failure. *Urban Data Service Rep*, *4*(4).

Colton, K. (1974). Computers and the police: Police departments and the new information technology. *Urban Data Service Rep.*, *6*(11).

Colton, K. (1978). *Police computer technology: Implementation and impact.* Lexington, MA: Lexington Books.

Colton, K. W. (1979). The impact and use of computer technology by the police. *Social Impacts of Computing*, *22*(1), 10-20.

Colton, K. W. (1980). Police and computer technology: The case of the San Diego computer-aided dispatch system. *Public Productivity Review*, *4*(1), 21-42.

Controlled Drugs and Substances Act, SC 1996, c 19, <https://canlii.ca/t/5657m> retrieved on 2024-01-27

Conway, S., & Westmarland, L. (2021). The blue wall of silence: police integrity and corruption. *Silence of organizations: how organizations cover up wrongdoings*, 105-132.

Cooper, R. (2023, November 6). OPP encourages residents to help fight crime with CAMSafe program. *CTV News*. https://barrie.ctvnews.ca/opp-encourages-residents-to-help-fight-crime-with-camsafe-program-1.6633358

Corbett, E., Denton, E., & Erete, S. (2023, October). Power and Public Participation in AI. In *Proceedings of the 3rd ACM Conference on Equity and Access in Algorithms, Mechanisms, and Optimization* (pp. 1-13).

Costanza-Chock, S., Raji, I. D., & Buolamwini, J. (2022, June). Who audits the auditors? Recommendations from a field scan of the algorithmic auditing ecosystem. In *Proceedings of the 2022 ACM Conference on Fairness, Accountability, and Transparency* (pp. 1571-1583).

Cox, J. (2022, February 8). NSO group gave pegasus spyware demo to the NYPD. *Vice*. https://www.vice.com/en/article/m7vp93/nso-group-pegasus-demo-nypd

Crow, M. S., Snyder, J. A., Crichlow, V. J., & Smykla, J. O. (2017). Community perceptions of police body-worn cameras: The impact of views on fairness, fear, performance, and privacy. *Criminal Justice and Behavior*, *44*(4), 589-610.

Criminal Code, RSC 1985, c C-46, <https://canlii.ca/t/565xr> retrieved on 2024-01-27

Crump, J. (2011). What are the police doing on Twitter? Social media, the police and the public. *Policy & internet*, *3*(4), 1-27.

Dafoe, A. (2022, February 14). AI Governance: Overview and Theoretical Lenses', in Justin B. Bullock, and others (eds), *The Oxford Handbook of AI Governance*. https://doi-org.myaccess.library.utoronto.ca/10.1093/oxfordhb/9780197579329.013.2, accessed 23 Jan. 2024.

Das, V. (2004). The signature of the state: the paradox of illegibility. In *Anthropology in the Margins of the State* (eds) V. Das & D. Poole, 225-52. New Delhi: Oxford University Press.

Brookings. (2021, September 13). *Data-driven policing's threat to our constitutional rights.* https://www.brookings.edu/articles/data-driven-policings-threat-to-our-constitutional-rights/

Data Justice Lab. (2021). Advancing civic participation in algorithmic decision-making: A guide for the public sector. https://datajusticelab.org/wp-content/uploads/2021/06/PublicSectorToolkit_english.pdf

Deflem, M, & Chicoine, S. (2014). History of technology in policing. In *Encyclopedia of Criminology and Criminal Justice* (Buinsma, G., & Weisburd, D., eds.), 2269-2277. Berlin: Springer.

DeGuire, P. (2024, January 10). Approval of high-risk technologies under the Toronto Police Services Board's Policy on the use of artificial intelligence technology. *Ontario Human Rights Commission*. https://www.ohrc.on.ca/en/news_centre/approval-high-risk-technologies-under-toronto-police-services-boards-policy-use-artificial

De Haes, S., & Van Grembergen, W. (2004). IT governance and its mechanisms. *Information Systems Control Journal, 1*.

Denham, E. (2012). Use of automated licence plate recognition technology by the Victoria Police Department. *OIPC BC*. https://www.oipc.bc.ca/investigation-reports/1480

de Secondat Montesquieu, C. (1977). *The spirit of laws*. Univ of California Press.

de Vries, P., & Schinkel, W. (2019). Algorithmic anxiety: Masks and camouflage in artistic imaginaries of facial recognition algorithms. *Big Data & Society*, *6*(1), 2053951719851532.

Dietz, T., & Stern, P.C., eds. (2008). Public Participation in Environmental Assessment and Decision Making. *Washington: The National Academies Press.*

Dignum, V. (2020, July 9). Responsibility and artificial intelligence', in Markus D. Dubber, Frank Pasquale, and Sunit Das (eds), *The Oxford Handbook of Ethics of AI* (2020; online edn, Oxford Academic). https://doi-org.myaccess.library.utoronto.ca/10.1093/oxfordhb/9780190067397.013.12, accessed 16 Jan. 2024.

Dufresne, P. (2022, August 8). Appearance before the standing committee on access to information, privacy and ethics (ETHI) on the study of device investigation tools used by the RCMP." *OPC*. https://www.priv.gc.ca/en/opc-actions-and-decisions/advice-to-parliament/2022/parl_20220808/

EDRi. (2022, April 6). *About Clearview AI's mockery of human rights, those fighting it, and the need for EU to intervene.* https://edri.org/our-work/we-need-to-talk-about-clearview-ai/

Emerson, K., Nabatchi, T., & Balogh, S. (2012). An integrative framework for collaborative governance. *Journal of Public Administration Research and Theory* 22(1): 1–29.

Ericson, R. V. (1989). Patrolling the facts: Secrecy and publicity in police work. *British Journal of Sociology*, 205-226.

Etter, L. (2021). *The Devil's Playbook: Big Tobacco, Juul, and the Addiction of a New Generation*. Crown.

Eubanks, V. (2018). *Automating inequality: How high-tech tools profile, police, and punish the poor*. St. Martin's Press.

EuroJust. (n.d.) *EuroJust: European Union Agency for Criminal Justice Cooperation*. https://www.eurojust.europa.eu/

Eurojust. (2019, September 29). Outline. https://rm.coe.int/3148-3-2-eurojust-joint-conf-outline-2019-en/1680979d60

Fadda, N., and Rotondo, F. (2020). What combinations of conditions lead to high performance of governance networks? A fuzzy set qualitative comparative analysis of 12 sardinian tourist networks. *International Public Management Journal*. doi:10.1080/10967494.2020.1755400.

Fagerberg, J., Martin, B. R., & Andersen, E. S. (Eds.). (2013). *Innovation studies: evolution and future challenges*. OUP Oxford.

Fanfair, R. (2023, November 1). Growing awareness of men's health. *TPS*. https://www.tps.ca/media-centre/stories/growing-awareness-of-mens-health/

Ferlie, E., Ashburner, L., Fitzgerald, L., & Pettigrew, A. (1996). The New Public Management in Action. Oxford University Press, Oxford.

Ferretti, T. (2022). An institutionalist approach to AI ethics: justifying the priority of government regulation over self-regulation. *Moral Philosophy and Politics*, *9*(2), 239-265.

Finnane, M. (1994). *Police and government: Histories of policing in Australia*. Oxford: Oxford University Press.

Fischer, F. (2012). Participatory governance: From theory to practice. In The Oxford Handbook of Governance. Oxford: OUP.

Forrest, M. (2022, September 30). RCMP's use of facial recognition extends well beyond Clearview AI. *Politico*. https://www.politico.com/news/2022/09/30/rcmps-facial-recognition-clearview-ai-00059639

Forst, B., & Manning, P. K. (1999). *The privatization of policing: Two views*. Georgetown University Press.

Foucault, M. (2002). *The birth of the clinic*. Routledge.

Freeze, C. (2022, November 27). RCMP's new privacy-protecting unit at risk of failing due to resource crunch, documents reveal. *The Globe and Mail*. https://www.theglobeandmail.com/canada/article-privacy-protecting-rcmp-unit/

Friedman, B., & Jánszky, E. G. (2020). Policing's Information Problem. *Tex. L. Rev.*, *99*, 1.

Friedman, B., Heydari, F., Isaacs, M., & Kinsey, K. (2022). Policing police tech: A soft law solution. *Berkeley Tech. LJ*, *37*, 701.

Frontline. (2023, September 25). Unleashing Justice: Canine Teams Steal the Show. *OPP News.* https://www.opp.ca/news/#/viewnews/6511ae6a14788

Fukuyama, F. (2013). What is governance?. *Governance*, *26*(3), 347-368.

Gabriel, I. (2020). Artificial intelligence, values, and alignment. *Minds and Machines* 30 (3): 411–37, https://doi.org/10.1007/s11023-020-09539-2.

Gates, K. (2006). Identifying the 9/11 faces of terror: The promise and problem of facial recognition technology. *Cultural Studies*, *20*(4-5), 417-440.

Gates, K. A. (2011). *Our biometric future: Facial recognition technology and the culture of surveillance* (Vol. 2). NYU Press.

Gillis, W., & Allen, K. (2020, March 1). OPP confirms use of controversial facial recognition tool clearview AI. *Toronto Star*. https://www.thestar.com/news/canada/opp-confirms-use-of-controversial-facial-recognition-tool-clearview-ai/article_8e8154ac-ddfc-51ca-9771-14919a946f3f.html

Gillis, W. (2022, February 28). 144 Toronto police officers signed up to use Clearview AI ‘mass surveillance’ tech. *Toronto Star*. https://www.thestar.com/news/gta/144-toronto-police-officers-signed-up-to-use-clearview-ai-mass-surveillance-tech/article_2cf7befc-7c22-5b47-bcb7-ab365d426569.html

Gilman, M. E. (2023). Democratizing AI: Principles for Meaningful Public Participation. *Data & Society*.

Goldstein, A.J., Harmon, L.D., & Lesk, A.B. (1971). Identification of human faces in *Proceedings of the IEEE*, 59(5), 748-760 doi: 10.1109/PROC

Government of Ontario. (July 30, 2021). *Policing in Ontario.* https://www.ontario.ca/page/policing-ontario

Government of Canada. (2022). *How national security and intelligence institutions engage with racialized communities.* https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2022-nstag-nsiirc-isnrccr/2022-nstag-nsiirc-isnrccr-en.pdf

Government of Canada. (2022, August 16). Part 3: Challenges of the current model. In *The Offices of the Information and Privacy Commissioners: The Merger and Related Issues.* https://www.justice.gc.ca/eng/rp-pr/csj-sjc/atip-

aiprp/ip/p7.html#:~:text=Commissioners%20with%20order%2Dmaking%20powers,should%20be%20interpreted%20and%20applied.

Government of Canada. (2022, August 16). *Strengthening the access to information act.* https://www.justice.gc.ca/eng/rp-pr/csj-sjc/atip-aiprp/atia-lai/p5.html

Government of Ontario. (January 8, 2024). *Ontario's trustworthy artificial intelligence (AI) framework.* https://www.ontario.ca/page/ontarios-trustworthy-artificial-intelligence-ai-framework

Graeber, D. (2012). Dead zones of the imagination: on violence, bureaucracy, and interpretive labour. *HaU: Journal of Ethnographic Theory* 2(2), 105-28.

Greene, K. (2022). AI Governance Multi-stakeholder Convening, in Justin B. Bullock, and others (eds), *The Oxford Handbook of AI Governance* (online edn, Oxford Academic). https://doi.org/10.1093/oxfordhb/9780197579329.013.6, accessed 23 Jan. 2024.

Grundmann, R. (2017). The problem of expertise in knowledge societies. *Minerva*, *55*(1), 25-48.

Gurinskaya, A. (2020). Predicting citizens' support for surveillance cameras. Does police legitimacy matter? *International journal of comparative and applied criminal justice*, *44*(1-2), 63-83.

Gurney, K. (2018). *An introduction to neural networks*. CRC press.

Gusterson, H. (2017). Homework: toward a critical ethnography of the university AES presidential address, 2017. *American Ethnologist*, 44(3), 435-450.

Haaretz. (2023, April 3). *U.S. used front company to buy Israeli NSO's spyware, report says.* https://www.haaretz.com/israel-news/security-aviation/2023-04-03/ty-article/u-s-used-front-company-to-buy-israeli-nsos-spyware-report/00000187-459d-df9b-a9d7-c59dfb490000

Hagemann, R., Huddleston J.S., & Thierer, A. (2018). Soft law for hard problems: The governance of emerging technologies in an uncertain future. *Colo. Tech. LJ*, *17*(37).

Haggerty, K.D., & Ericson, R.V. (2000). The surveillant assemblage. *British Journal of Sociology, 51*(4), 605-622.

Harris, C.J. (2007). The police and soft technology: How information technology contributes to police decision making. In Byrne, J.M., & Rebovich, D.J. (eds.), pp. 153-184. *The new technology of crime, law and social control*. Ohio: Criminal Justice Press.

Hawley, K. (2012). *Trust: A very short introduction*. OUP Oxford.

Haynes, P. (2003). *Managing complexity in the public services*. Maidenhead: Open University Press.

Heen, M. S., Lieberman, J. D., & Miethe, T. D. (2018). The thin blue line meets the big blue sky: Perceptions of police legitimacy and public attitudes towards aerial drones. *Criminal Justice Studies, 31*(1), 18-37.

Heikkilä, M. (2022, May 24). The walls are closing in on Clearview AI. *MIT Technology Review*. https://www.technologyreview.com/2022/05/24/1052653/clearview-ai-data-privacy-uk/

Helm, J. M., Swiergosz, A. M., Haeberle, H. S., Karnuta, J. M., Schaffer, J. L., Krebs, V. E., Spitzer, A. I., & Ramkumar, P. N. (2020). Machine learning and artificial intelligence: Definitions, applications, and future directions. *Current Reviews in Musculoskeletal Medicine, 13*(1), 69–76. https://doi.org/10.1007/s12178-020-09600-8

Helmer, A. (2016, September 1). Ottawa police introduce automatic license plate scanners. *Ottawa Citizen*. https://ottawacitizen.com/news/local-news/ottawa-police-introduce-automatic-licence-plate-scanners

Henriksen, A., Enni, S., & Bechmann, A. (2021). Situated accountability: Ethical principles, certification standards, and explanation methods in applied AI. In *Proceedings of the 2021 AAAI/ACM Conference on AI, Ethics, and Society* (pp. 574-585).

Hermansson, H.M.L. (2016). Disaster management collaboration in Turkey: Assessing progress and challenges of hybrid network governance. *Public Administration 94*(2), 333–349.

Heverin, T., & Zach, L. (2010) Twitter for city police department information sharing. *Proceedings of the American Society for Information Science and Technology* 47(1), 1–7.

Hill, K. (2020, Jan 18). The secretive company that might end privacy as we know it. *New York Times*.https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html

Hill, K., & Dance, G.J.X. (2020, February 10). Clearview's facial recognition app is identifying child victims of abuse. *The New York Times.* Clearview's Facial Recognition App Is Identifying Child Victims of Abuse - The New York Times (nytimes.com)

Hill, D., O'Connor, C. D., & Slane, A. (2022). Police use of facial recognition technology: The potential for engaging the public through co-constructed policy-making. *International Journal of Police Science & Management, 24*(3), 325-335.

Hobson, Z., Yesberg, J. A., Bradford, B., & Jackson, J. (2021). Artificial fairness? Trust in algorithmic police decision-making. *Journal of experimental criminology*, 1-25.

Hoffman, A. (2023, November 8). Why self-regulation is best for artificial intelligence. *The Hill*.https://thehill.com/opinion/4300288-why-self-regulation-is-best-for-artificial-intelligence/#:~:text=In%20the%20absence%20of%20self,the%20need%20for%20burdensome%20regimes.

Hough, M. (2010). Policing, new public management and legitimacy. In *The new public leadership challenge* (pp. 70-84). Palgrave Macmillan, London.

Howlett, M., & Ramesh, M. (2014). The two orders of governance failure: Design mismatches and policy capacity issues in modern governance. *Policy and Society*, *33*(4), 317-327.

Hueglin, T. O. (2021). *Federalism in Canada: Contested Concepts and Uneasy Balances*. University of Toronto Press.

Huey, L., Ferguson, L., & Schulenberg, J. L. (2023). *The Wicked Problems of Police Reform in Canada* (1st edition., Vol. 1). Routledge. https://doi.org/10.4324/9781003296447

Hughes, T.P. (1987). The evolution of large technological systems. In Wiebe E. Bijker, Thomas P. Hughes, and Trevor Pinch, eds., *The Social Construction of Technological Systems: New Directions in the Sociology and History of Technology*. pp. 45-76.

Hughes, T.P. (2000). Technological momentum. In Albert Teich, ed., *Technology and the Future*, 8th edn.

Hughes, T.P. (1994). Technological momentum. In Merritt Roe Smith and Leo Marx, ed., *Does Technology Drive History?: The Dilemma of Technological Determinism*, Massachusetts Institute of Technology. pp. 101–113

Hull, E. (2012). Paperwork and the contradictions of accountability in a South African hospital. *Journal of the Royal Anthropological Institute* 18, 613-32.

Hyatt, J. M., Mitchell, R. J., & Ariel, B. (2017). The effects of a mandatory body-worn camera, policy on officer perceptions of accountability, oversight, and departmental culture. *Vill. L. Rev.*, *62*, 1005.

Ingrams, A. (2017). Managing governance complexity and knowledge networks in transparency initiatives: the case of police open data, *Local Government Studies*, 43(3), 364-387, DOI: 10.1080/03003930.2017.1294070

Ingrams, A. (2017). The legal-normative conditions of police transparency: A configurational approach to open data adoption using qualitative comparative analysis. *Public Administration*, *95*(2), 527-545.

Isaac, W. S. (2017). Hope, hype, and fear: the promise and potential pitfalls of artificial intelligence in criminal justice. *Ohio St. J. Crim. L.*, *15*, 543.

Isett, K. R., Mergel, I. A., LeRoux, K., Mischen, P. A., & Rethemeyer, R. K. (2011). Networks in public administration scholarship: Understanding where we are and where we need to go. *Journal of public administration research and theory*, *21*(suppl_1), i157-i173.

Jackson, B. A. (2015). *Strengthening trust between police and the public in an era of increasing transparency*. Arlington, VA: Rand Corporation.

Jackson, J., & Bradford, B. (2010). What is trust and confidence in the police? *Policing: A Journal of Policy and Practice*, *4*(3), 241-248.

Jasanoff, S. (1990). *The fifth branch: science advisers as policymakers*. Harvard University Press.

Jasanoff, S. (2015). Future imperfect: Science, technology, and the imaginations of modernity. *Dreamscapes of modernity: Sociotechnical imaginaries and the fabrication of power*, 1-33.

Jaynes, A. (2020, February 14). The end of anonymity? Facial recognition app used by police raises serious concerns, say privacy advocates | *CBC Radio*. https://www.cbc.ca/radio/thecurrent/the-current-for-jan-21-2020-1.5434328/the-end-of-anonymity-facial-recognition-app-used-by-police-raises-serious-concerns-say-privacy-advocates-1.5435278

Joh, E. E. (2019). The consequences of automating and deskilling the police. *UCLA L. Rev. Discourse*, *67*, 133.

Johnson, D.R. (1981). *American law enforcement: A history*. St. Louis, MI: Forum Press.

Jones, T., Newburn, T., & Smith, D. J. (1996). Policing and the idea of democracy. *British Journal of Criminology, 36*(2), 182–198. https://doi.org/10.1093/oxfordjournals.bjc.a014081

Katzenbach, N. (1967). *The challenge of crime in a free society: A report by the President's Commission on Law Enforcement and Administration of Justice*. Washington, D.C.: United States Government Printing Office.

Kazansky, B., & Milan, S. (2021). "Bodies not templates": Contesting dominant algorithmic imaginaries. *New Media & Society, 23*(2), 363-381.

Keen, M. F. (1992). The freedom of information act and sociological research. *The American Sociologist*, *23*(2), 43-51.

Kelly, P. (2022, October). Use and impacts of facial recognition technology. *ETHI*. https://www.ourcommons.ca/committees/en/ETHI/StudyActivity?studyActivityId=11566271

Kenyon, G. (2022, February 24). The man who studies the spread of ignorance. *BBC Future*. https://www.bbc.com/future/article/20160105-the-man-who-studies-the-spread-of-ignorance

Kitchin, R., & Dodge, M. (2011). Code/space: Software and everyday life. Cambridge: MIT Press.

Klein, H. K., & Kleinman, D. L. (2002). The social construction of technology: Structural considerations. *Science, Technology, & Human Values*, *27*(1), 28-52.

Klijn, E. H., & Koppenjan, J. (2014). Complexity in governance network theory. *Complexity, Governance & Networks*, *1*(1), 61-70.

Kline, S.J. and Rosenberg, N. (1986) An overview of innovation. In: Landau, R. and Rosenberg, N., Eds., The Positive Sum Strategy: Harnessing Technology for Economic Growth, National Academy Press, Washington DC, 275-307.

Kochel, T. R., & Skogan, W. G. (2021). Accountability and transparency as levers to promote public trust and police legitimacy: Findings from a natural experiment. *Policing: An International Journal*, *44*(6), 1046-1059.

Koen, M. C., & Mathna, B. (2019). Body-worn cameras and internal accountability at a police agency. *American Journal of Qualitative Research*, *3*(2), 1-22.

Koepke, J. E. (1999). The failure to breach the blue wall of silence: The circling of the wagons to protect police perjury. *Washburn LJ*, *39*, 211.

Konikoff, D. (2022). Digital Oversight: How Social Media Users "Oversee" Police Misconduct in North America.

Koningisor, C. (2023). Police secrecy exceptionalism. *Colum. L. Rev.*, *123*, 615.

Koper, C. S., & Lum, C. (2019). Critic: The limits of police technology. In D. Weisburd & A. A. Braga (Eds.), *Police Innovation: Contrasting Perspectives* (pp. 517–543). Cambridge: Cambridge University Press.

Kostka, G., Steinacker, L., & Meckel, M. (2023). Under big brother's watchful eye: Cross-country attitudes toward facial recognition technology. *Government Information Quarterly*, *40*(1), 101761.

Kourany, J., & Carrier, M. (Eds.). (2020). *Science and the production of ignorance: When the quest for knowledge is thwarted*. Mit Press.

KPMG. (2018, December 6). Evaluation of the canada accelerator and incubator program (CAIP). *National Research Council*. https://nrc.canada.ca/sites/default/files/2019-04/caip_final_report_6.12.18.pdf

Kroezen, M., van Dijk, L., Groenewegen, P. P., & Francke, A. L. (2013). Knowledge claims, jurisdictional control and professional status: the case of nurse prescribing. *PLoS One*, *8*(10), e77279.

Kurenkov, A. (2022, January 15). The messy history of facial recognition company clearview AI. *Last Week in AI.* https://lastweekin.ai/p/the-messy-history-and-many-legal

Kuziemski, M., & Misuraca, G. (2020). AI governance in the public sector: Three tales from the frontiers of automated decision-making in democratic settings. *Telecommunications Policy*, *44*(6), 101976.

Kwon, J. (2023). *Misconduct Mismanagement: Independent Oversight, Accountability, and the Rule of Law* (Doctoral dissertation).

Law, J. (2009). Actor network theory and material semiotics. *The New Blackwell Companion to Social Theory, 3*, 141–158.

Lazar, Seth, (2022). Power and AI: nature and justification, In Justin B. Bullock, and others (eds), *The Oxford Handbook of AI Governance* (online edn, Oxford Academic). https://doi-org.myaccess.library.utoronto.ca/10.1093/oxfordhb/9780197579329.013.12, accessed 23 Jan. 2024.

Lazzaro, S. (2023, November 7). Cops are falling in love with AI, and it's much deeper than facial recognition. *Fortune*. https://fortune.com/2023/11/07/police-ai-facial-recognition-cop-con/

Lee, S. (2022). When tensions become opportunities: Managing accountability demands in collaborative governance, *Journal of Public Administration Research and Theory*, 32(4), 641-655. https://doi.org/10.1093/jopart/muab051

Legal Aid NYC. (n.d.). *Clearview AI disclosure.* https://legalaidnyc.org/wp-content/uploads/2021/04/Legal-Aid-Index-No.-158526-2020-Disclosure.pdf

Lemieux, F. (2011). Information technology and criminal intelligence: A comparative perspective. In *Technocrime: Technology, crime and social control* (Leman-Langlois, S. ed), p. 139-168. New York, NY: Routledge.

Levi-Faur, D. (ed.) (2012). *The Oxford Handbook of Governance* (2012; online edn, Oxford Academic), https://doi.org/10.1093/oxfordhb/9780199560530.001.0001, accessed 22 Jan. 2024.

Li, M. (2017). Collaborative governance and partnerships in policing. *Open Journal of Social Sciences*, *5*(12), 50-58.

Liu, A. (2020). Blue wall of silence: degradation of accountability. Dissertation.

Luscombe, A., & Walby, K. (2017). Theorizing freedom of information: The live archive, obfuscation, and actor-network theory. *Government Information Quarterly*, *34*(3), 379-387.

Luscombe, A., Walby, K., & Lippert, R. K. (2017). Brokering access beyond the border and in the wild: Comparing freedom of information law and policy in Canada and the United States. *Law & Policy*, *39*(3), 259-279.

Lvovsky, A. (2021). Rethinking police expertise. *Yale LJ*, *131*, 475.

Mac, R., Haskins, C., & McDonald, L. (2020, February 28). Clearview AI's facial recognition tech is being used by the Justice Department, ICE, and the FBI. *BuzzFeed News*. https://www.buzzfeednews.com/article/ryanmac/clearview-ai-fbi-ice-global-law-enforcement

Maguire, E.R., & King, W.R. (2004). Trends in the policing industry. *The ANNALS of the American Academy of Political and Social Science, 593*(1), 15-41.

Manes, J. (2019). Secrecy & evasion in police surveillance technology. *Berkeley Technology Law Journal, 34*(2), 503-566.

Mann, M. (2017). New public management and the 'business' of policing organised crime in Australia. *Criminology & Criminal Justice*, *17*(4), 382-400.

Manning, P. K. (1992). Information technologies and the police. *Crime and Justice, 15*, 349–398. https://doi.org/10.1086/449197

Manning, P. K. (2016). *Democratic policing in a changing world.* Routledge.

Manwaring-White, S. (1983). *The policing revolution: Police technology, democracy and liberty in Britain*. Brighton, UK: Harvester Press.

Mason, D., Hillenbrand, C., & Money, K. (2014). Are informed citizens more trusting? Transparency of performance data and trust towards a British police force. *Journal of Business Ethics*, *122*, 321-341.

Mateescu, A., & Rosenblat, A. (2016). Dreams of accountability, guaranteed surveillance: The promises and costs of body-worn cameras. *Surveillance & Society*, *14*(1), 122-127.

Mathur, N. 2016. *Paper tiger: law, bureaucracy, and the developmental state in Himalayan India*. Cambridge: University Press.

Mawby, R. C., & Worthington, S. (2002). Marketing the police–from a force to a service. *Journal of Marketing Management*, *18*(9-10), 857-876.

Mawby, R. C. (2010). Police corporate communications, crime reporting and the shaping of policing news. *Policing and Society*, *20*(1), 124-139.

McDonough, A. (2023, April 13). NYPD may be violating police surveillance transparency law. *City & State New York.* https://www.cityandstateny.com/policy/2023/04/nypd-may-be-violating-police-surveillance-transparency-law/385173/

McFarlane, A. (2001). When Inclusion Leads to Exclusion: The Uncharted Terrain of Community Participation in Economic Development. *Brooklyn Law Review,* 66 (2001): 861–931.

Ministry of Government and Consumer Services. (2018). *Freedom of information and protection of privacy manual.* https://files.ontario.ca/books/mgcs-foi-privacy-manual-en-2021-09-02.pdf

Ministry of Public Safety and Solicitor General. (2006, November 9). Government and police launch new crime-fighting tool." *British Columbia.* https://archive.news.gov.bc.ca/releases/news_releases_2005-2009/2006pssg0054-001342.htm

Ministry of the Solicitor General. (2021, November 4). Policing and community safety. *Ontario.* https://www.ontario.ca/page/policing-and-community-safety

Mitcham, C., & Schatzberg, E. (2009). Defining technology and the engineering sciences. In *Philosophy of Technology and Engineering Sciences* (pp. 27-63). North-Holland.

Mitchell, D. (2023, May 29). Hamilton police expects to use drones 'more frequently' over time. *Global News*. https://globalnews.ca/news/9729616/hamilton-police-drone-use-increasing/

Morrell, K., & Bradford, B. (2018). *Policing and public management: governance, vices and virtues*. Routledge.

Morton, D. R. (2018). Improving police transparency and accountability in violent encounters with African Americans. *Journal of African American Studies*, *22*, 125-138.

National Security Transparency Advisory Group. (2022). How National Security and Intelligence Institutions Engage with Radicalized Communities. *Ministry of Public Safety Canada*.

NEC. (2022, May 12). *A brief history of facial recognition.* https://www.nec.co.nz/market-leadership/publications-media/a-brief-history-of-facial-recognition/

Newkirk, A. B. (2010). The rise of the fusion-intelligence complex: A critique of political surveillance after 9/11. *Surveillance & Society*, *8*(1), 43-60.

New York Policing Project. (2023, December 15). The transparency New Yorkers deserve: How city council must hold NYPD to account. *New York University School of Law*. https://www.policingproject.org/news-main/2023/12/15/our-testimony-to-the-new-york-city-council-on-nypds-transparency-failures-and-necessary-changes-to-the-post-act-dakfe

Ng, A. (2020, February 26). Clearview AI's entire client list stolen in data breach. *CNET*. https://www.cnet.com/news/privacy/clearview-ai-had-entire-client-list-stolen-in-data-breach/#google_vignette

No author. (2023, October 13). Perth County RIDE Check Catches More Than Impaired Driver. *OPP News.* https://www.opp.ca/news/#/viewnews/65294b56e9b0a

Nuberger, A. (2018). Hard law or soft law–does it matter? Distinction between different sources of international law in the jurisprudence of the ECtHR. In *The European Convention on Human Rights and General International Law* (pp. 41-58).

Nunn, S. (2001). Police technology in cities: Changes and challenges. *Technology in Society, 23*(1), 11–27. https://doi.org/10.1016/s0160-791x(00)00033-6

Nunn, S. (2001). Police information technology: Assessing the effects of computerization on urban police functions. *Public Administration Review, 61*(2), 221-234.

NYCC. (2020). *Legislation details – POST act.* https://legistar.council.nyc.gov/LegislationDetail.aspx?ID=3343878&GUID=996ABB2A-9F4C-4A32-B081-D6F24AB954A0

ODS. (2021, May 6). Consultation: Ontario's trustworthy artificial intelligence (AI) framework." *Ontario*. https://www.ontario.ca/page/ontarios-trustworthy-artificial-intelligence-ai-framework-consultations

ODS (2022, January 7). Principles for ethical use of AI." *Ontario*. https://www.ontario.ca/page/beta-principles-ethical-use-ai-and-data-enhanced-technologies-ontario

Oelschlaeger, M. (1979). The myth of the technological fix. *The Southwestern Journal of Philosophy, 10*(1), 43-53.

O'Connor, C. D. (2017). The police on Twitter: image management, community building, and implications for policing in Canada. *Policing and Society, 27*(8), 899-912.

O'Hara, K. (2012, June). Transparency, open data and trust in government: Shaping the infosphere. In *Proceedings of the 4th annual ACM web science conference* (pp. 223-232).

Office of the Privacy Commissioner of Canada. (2020, July 6). *Clearview AI ceases offering its facial recognition technology in Canada.* https://priv.gc.ca/en/opc-news/news-and-announcements/2020/nr-c_200706/

Office of the Privacy Commissioner of Canada. (2021, June 10). *Police use of facial recognition technology in Canada and the way forward*. https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/202021/sr_rcmp/#fn1

Office of the Privacy Commissioner of Canada. (2022a, May 2). *Privacy guidance on facial recognition for police agencies*. https://www.priv.gc.ca/en/privacy-topics/surveillance/police-and-public-safety/gd_fr_202205/

Office of the Privacy Commissioner of Canada. (2022b, May 2). *Recommended legal framework for police agencies' use of facial recognition*. https://priv.gc.ca/en/opc-actions-and-decisions/advice-to-parliament/2022/s-d_prov_20220502/

Ontario. (n.d.). Freedom of Information request. *Ontario*. https://www.ontario.ca/page/freedom-information-request

Ontario (n.d.). *Chapter 5: Exemptions and Exclusions | Freedom of Information and Protection of Privacy Manual*. (n.d.). https://www.ontario.ca/document/freedom-information-and-protection-privacy-manual/chapter-5-exemptions-and-exclusions

Ontario. (2019, March 26). *Comprehensive Ontario Police Services Act, 2019, S.O. 2019, c. 1 - Bill 68.* https://www.ontario.ca/laws/statute/s19001

Ontario Digital Service. (n.d.) Overview. https://www.ontario.ca/page/ontario-digital-service.

OPC. (2021, February 2). Joint investigation of clearview AI, Inc. by the office of the privacy commissioner of Canada, the commission d'accès à l'information du Québec, the information and privacy commissioner for British Columbia, and the information privacy commissioner of Alberta." https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2021/pipeda-2021-001/

OPC. (2021, June 10). Police use of facial recognition technology in Canada and the way forward. https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/202021/sr_rcmp/#toc1

OPC. (2022, November 7). Key issues related to privacy. https://www.priv.gc.ca/en/privacy-and-transparency-at-the-opc/proactive-disclosure/opc-parl-bp-incoming/pd_20220627/6b_issues/

OPC. (2021, April 14). Consulting with the office of the privacy commissioner's government advisory directorate. https://www.priv.gc.ca/en/for-federal-institutions/privacy-act-bulletins/pab_20210414/

Oslo Manual, O. E. C. D. (2005). Guidelines for collecting and interpreting innovation data. https://www.oecd-ilibrary.org/science-and-technology/oslo-manual_9789264013100-en

Otway, H. (1992). Public wisdom, expert fallibility: Toward a contextual theory of risk.

Paasche, T. F. (2013). 'The softer side of security': The role of social development in Cape Town's policing network. *Geoforum*, *45*, 259-265.

Paraskevopoulou, E. (2012). Non-technological regulatory effects: Implications for innovation and innovation policy. *Research Policy*, *41*(6), 1058-1071.

Pasquale, F. (2015). *The black box society: The secret algorithms that control money and information*. Harvard University Press.

Peters, B. G. (2015). State failure, governance failure and policy failure: Exploring the linkages. *Public Policy and Administration*, *30*(3-4), 261-276.

Pinch, T. J., & Bijker, W. E. (1984). The social construction of facts and artefacts: Or how the sociology of science and the sociology of technology might benefit each other. *Social Studies of Science*, *14*(3), 399–441. http://www.jstor.org/stable/285355

Pinkerton Consulting & Investigations. (n.d.). *Our history.* https://pinkerton.com/our-story/history

Poland, T. (2022, October 12). New phrasebook introduces RCMP officers to Inuit languages. *RCMP Gazette*. https://www.rcmp-grc.gc.ca/en/gazette/new-phrasebook-introduces-rcmp-officers-inuit-languages?h

Police Brutality Center. (2023, September 18). *What is police reform? | Police Brutality Center*. https://policebrutalitycenter.org/what-is-police-reform/

Police Services Act. "O. Reg. 3/99 Adequacy and Effectiveness of Police Services."https://www.ontario.ca/laws/regulation/990003[MOU1]

Pollitt, C. (1993). *Managerialism and the public services: The Anglo-American experience*. Oxford, UK: Blackwell.

Poluha, E., & Rosendahl, M. (2012). *Contesting 'good' governance: Crosscultural perspectives on representation, accountability and public space*. Routledge.

Porumbescu, G. (2017). Linking transparency to trust in government and voice. *The American Review of Public Administration*, *47*(5), 520-537.

Powers Jr, J. J. (2000). Eroding the blue wall of silence: The need for an internal affairs privilege of confidentiality. *Suffolk J. Trial & App. Advoc.*, *5*, 19.

Prenzler, T., & den Heyer, G. (Eds.) (2015). *Civilian oversight of police: Advancing accountability in law enforcement.* Routledge.

President's Task Force on Century Policing. (2015). *Final report of the president's task force on 21st century policing,* Washington, DC: Office of Community Oriented Policing Services.

Proctor, R. N., & Schiebinger, L. (2008). Agnotology: The making and unmaking of ignorance. California: Stanford University Press.

Provan, K. G., & Kenis, P. (2008). Modes of network governance: Structure, management, and effectiveness. *Journal of Public Administration Research and Theory*, *18*(2), 229-252.

Purdy, J.M. (2012). A framework for assessing power in collaborative governance process. *Public Administration Review 72*(3), 409–417.

Ran, B., and H. Qi. (2019). The entangled twins: Power and trust in collaborative governance. *Administration & Society* 51(4), 607–636.

Raviv, S. (2020, January 21). The secret history of facial recognition. *Wired.* https://www.wired.com/story/secret-history-facial-recognition/

RCMP. (2013, August 30). *Contract policing.* https://www.rcmp-grc.gc.ca/ccaps-spcca/contract-eng.htm

RCMP. (2021, June 10). Response to the report by the office of the privacy commissioner into the RCMP's use of clearview AI. https://www.rcmp-grc.gc.ca/en/news/2021/response-the-report-the-office-the-privacy-commissioner-the-rcmps-use-clearview-ai

RCMP. (2022, August 24). Access to information and privacy. https://www.rcmp-grc.gc.ca/en/access-information-and-privacy

RCMP. (2022, December 5). Annual report to parliament 2021-2022 on the administration of the privacy act. https://www.rcmp-grc.gc.ca/en/annual-report-parliament-2021-2022-the-administration-the-privacy-act

RCMP. (2023, October 20). Annual report to parliament on the administration of the privacy act 2022-2023.https://www.crcc-ccetp.gc.ca/en/annual-report-parliament-administration-privacy-act-2022-2023

Reed, G., Hendlin, Y., Desikan, A., MacKinney, T., Berman, E., & Goldman, G. T. (2021). The disinformation playbook: how industry manipulates the science-policy process—and how to restore scientific integrity. *Journal of Public Health Policy*, *42*, 622-634.

Reese, H. (2022). What happens when police use AI to predict and prevent crime? *JSTOR Daily*. https://daily.jstor.org/what-happens-when-police-use-ai-to-predict-and-prevent-crime/

Reiner, R. (2010). *The politics of the police*. OUP Oxford.

Rhodes, R. A. W. (1996). The new governance: governing without government. *Political studies*, *44*(4), 652-667.

Riles, A. 2001. *The network inside out.* Ann Arbor: University of Michigan Press.

Ritchie, K. L., Cartledge, C., Growns, B., Yan, A., Wang, Y., Guo, K., ... & White, D. (2021). Public attitudes towards the use of automatic facial recognition technology in criminal justice systems around the world. *PloS one*, *16*(10), e0258241.

Robertson, K., Khoo, C., & Song, Y. (2020). To surveil and predict: A human rights analysis of algorithmic policing in Canada. Citizen Lab and International Human Rights Program, University of Toronto.

Robertson, K., Thomasen, K., & Dunn, S. (2022, January 25). Algorithmic policing policies through a human rights and substantive equality lens. *U of T Centre for Ethics*. https://www.youtube.com/watch?v=qzKuC1y6s_8

Rogger, D., & Lewis, C. (2018, January 4). How does anthropology help us understand bureaucracy? *World Bank Blogs.* https://blogs.worldbank.org/governance/how-does-anthropology-help-us-understand-bureaucracy-0

Rose, J. A., & Lacher, D. C. (2017). *Managing public safety technology : deploying systems in police, courts, corrections, and fire organizations* (First edition.). Routledge. https://doi.org/10.4324/9781315397863

Rosenbaum, D. P., & Lurigio, A. J. (1994). An inside look at community policing reform: Definitions, organizational changes, and evaluation findings. *Crime & Delinquency*, *40*(3), 299-314.

Rosner, L. (Ed.). (2013). *The technological fix: how people use technology to create and solve problems*. Routledge.

Rossler, M. T., & Terrill, W. (2012). Police responsiveness to service-related requests. *Police Quarterly*, *15*(1), 3-24.

R. *v.* Cornell, 2010 SCC 31, [2010] 2 S.C.R. 142.

Sakiyama, M., Miethe, T. D., Lieberman, J. D., Heen, M. S., & Tuttle, O. (2017). Big hover or big brother? Public attitudes about drone usage in domestic policing activities. *Security Journal*, *30*, 1027-1044.

Sandefur, R. L. (2015). Elements of professional expertise: Understanding relational and substantive expertise through lawyers' impact. *American Sociological Review*, *80*(5), 909-933.

Saulnier, A. & Konikoff, D. (2023, February 7). AI draft procedure public response Saulnier and Konikoff." *TPS AI Draft Procedure Public Responses*. https://www.tps.ca/services/resource-centre/ai-draft-procedure-public-response-saulnier-and-ko/

Savage, A., & Hyde, R. (2014). Using freedom of information requests to facilitate research. *International Journal of Social Research Methodology*, *17*(3), 303-317.

Scassa, T. (2021). Administrative law and the governance of automated decision making: A critical look at Canada's directive on automated decision making. *UBCL Rev.*, *54*, 251.

Schafer, J.A. (2013). The role of trust and transparency in the pursuit of procedural and organisational justice. *Journal of Policing, Intelligence and Counter Terrorism,* 8(2), 131-143, DOI: 10.1080/18335330.2013.821738

Schellewald, A. (2022). Theorizing "stories about algorithms" as a mechanism in the formation and maintenance of algorithmic imaginaries. *Social Media & Society*, *8*(1), 20563051221077025.

Schneider, C.J., & Laming, E. (2021, January 31). A looming monopoly in Canadian justice. *Hamilton Spectator.* https://www.thespec.com/opinion/contributors/a-looming-monopoly-in-canadian-justice/article_5acbfbcd-3898-56e8-be17-e5dfd91cbdfc.html

Schwabe, W., Davis, L.M., & Jackson, B.A. (2000). *Challenges and choices for crime-fighting technology: Federal support of state and local law enforcement*. Santa Monica, CA: RAND.

Seglins, D., Braga, M., & Cullen, C. (2017, April 5). RCMP reveals use of secretive cellphone surveillance technology for the first time. *CBC News*. https://www.cbc.ca/news/science/rcmp-surveillance-imsi-catcher-mdi-stingray-cellphone-1.4056750

Selwyn, N., & Gallo Cordoba, B. (2022). Australian public understandings of artificial intelligence. *AI & SOCIETY*, *37*(4), 1645-1662.

Shevlane, T., Farquhar, S., Garfinkel, B., Phuong, M., Whittlestone, J., Leung, J., ... & Dafoe, A. (2023). Model evaluation for extreme risks. *arXiv preprint arXiv:2305.15324*.

Siems, E., Strandburg, K. J., & Vincent, N. (2022). Trade secrecy and innovation in forensic technology. *Hastings LJ*, *73*, 773.

Simmons, K. C. (2007). The politics of policing: Ensuring stakeholder collaboration in the federal reform of local law enforcement agencies. *J. Crim. L. & Criminology*, *98*, 489.

Sirovich, L., & Kirby, M. (1987). Low-dimensional procedure for the characterization of human faces. *Josa a*, *4*(3), 519-524.

Skogan, W. G. (2014). Why reforms fail. In *Police Reform from the Bottom Up* (pp. 144-155). Routledge.

Solicitor General. (2021, January 19). Ontario building a more connected justice sector. *Ontario*. https://news.ontario.ca/en/release/60006/ontario-building-a-more-connected-justice-sector

Solomon, H. (2022, August 16). RCMP still interested in facial recognition software. *IT World Canada*. https://www.itworldcanada.com/article/rcmp-still-interested-in-facial-recognition-software/498312

Soss, J., & Weaver, V. (2017). Police are our government: Politics, political science, and the policing of race–class subjugated communities. *Annual Review of Political Science*, *20*, 565-591.

Spitzer, S., & Scull, A. T. (1977). Privatization and capitalist development: The case of the private police. *Social Problems*, *25*(1), 18–29. https://doi.org/10.2307/800464

Spitzer, S., & Scull, A. T. (1977). Social control in historical perspective: from private to public responses to crime. *Corrections and Punishment*, 265-286.

Stalcup, M. (2013). Interpol and the emergence of global policing. In *Policing and Contemporary Governance: The Anthropology of Police in Practice* (Garriot, W., ed.), pp. 231-261. New York, NY: Palgrave Macmillan.

Stardust, Z., Gillett, R., & Albury, K. (2023). Surveillance does not equal safety: Police, data and consent on dating apps. *Crime, Media, Culture*, *19*(2), 274-295.

Stone, C. E., & Ward, H. H. (2000). Democratic policing: A framework for action. *Policing & Society, 10*(1), 11–45. https://doi.org/10.1080/10439463.2000.9964829

Stone, K. E. (2018). Smart policing and the use of body camera technology: unpacking South Africa's tenuous commitment to transparency. *Policing: A Journal of Policy and Practice*, *12*(1), 109-115.

Strathern, M. (2000). Introduction: new accountabilities. In *Audit Cultures: Anthropological Studies in Accountability, Ethics and the Academy* (ed.) M. Strathern, 1-18. New York: Routledge.

Sunshine, J., & Tyler, T. R. (2003). The role of procedural justice and legitimacy in shaping public support for policing. *Law & Society Review*, *37*(3), 513-548.

Sweeting, F., Cole, T., & Hills, P. (2022). Is the blue wall of silence a fallacy in cases of police sexual misconduct?. *International Journal of Police Science & Management*, *24*(3), 285-297.

Thomson, A. M., & Perry, J. L. (2006). Collaboration processes: Inside the black box. *Public Administration Review*, *66*, 20–32.

Tombs, S. and Whyte, D. (eds.) (2003). *Unmasking the Crimes of the Powerful: scrutinizing states and corporations*. New York: Peter Lang.

TPS. (n.d.). *Business with the Toronto police*. https://www.tps.ca/services/do-business-service/

TPS. (n.d.). *Information access.* https://www.tps.ca/organizational-chart/information-technology-command/information-management/information-access/

TPS. (n.d.). *Freedom of information requests.* https://www.tps.ca/services/freedom-information-request/

TPS. (2017, January). *Action plan: The way forward – Modernizing community safety in Toronto*. https://www.toronto.ca/legdocs/mmis/2017/ex/bgrd/backgroundfile-103581.pdf

TPS. (2021, January 27). 04-46 closed circuit television (CCTV). *TPS Procedures*. https://www.tps.ca/service-procedures/

TPS. (2022, July 6). *15-20 body worn camera.* https://www.tps.ca/service-procedures/

TPS. (2022, July 6). *16-07 collection, analysis and reporting of race and identity-based data.* https://www.tps.ca/service-procedures/

TPS. (2023, June 22). *02-18 executing a search warrant.* https://www.tps.ca/media/procedures/0922b9d5-cc5c-4f14-8ad7-355be76b623e.pdf

TPS. (2022, September 26). *15-17 In-car camera system*. https://www.tps.ca/service-procedures/

TPSB. (2019, May 30). Vendor award - Facial recognition system. In *Public Meeting Minutes.* https://tpsb.ca/jdownloads-categories/send/54-2019/613-may-30

TPSB. (n.d.). *Purchasing by-law.* https://www.tpsb.ca/jdownloads-categories?task=download.send&id=616:purchasing-by-law&catid=37

TPS Detective Operations. (2020, March 27). Toronto police service clearview AI: Usage, review & analysis. FOI disclosure.

Treasury Board Secretariat. (2020, June 18). Policy on privacy protection. *Government of Canada*. https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=12510

Treasury Board Secretariat. (n.d.). Directive on automated decision-making. *Government of Canada.* https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=32592

Tregle, B., Nix, J., & Pickett, J. (2022). Body-worn cameras and transparency: Experimental evidence of inconsistency in police executive decision-making, *Justice Quarterly, 39*(3), 455-477, DOI: 10.1080/07418825.2020.1821086

Trigaux, R. (2005, September 9). Cameras scanned fans for criminals. *Tampa Bay Times.* https://www.tampabay.com/archive/2001/01/31/cameras-scanned-fans-for-criminals/

Tsebelis, G. (2011). Veto player theory and policy change: An introduction. *Reform Processes and Policy Change: Veto Players and Decision-Making in Modern Democracies*, 3-18.

Tunney, C. (2020, February 27). RCMP acknowledges using facial recognition technology, but won't say where. *CBC News.* https://www.cbc.ca/news/politics/clearview-ai-rcmp-facial-recognition-1.5479098

Tunney, C. (2020, February 28). RCMP's use of clearview AI facial recognition technology under investigation. *CBC News.* https://www.cbc.ca/news/politics/clearview-ai-rcmp-facial-recognition-1.5479673

Tunney, C. (2020, March 4). RCMP denied using facial recognition technology - then said it had been using it for months. *CBC News.* https://www.cbc.ca/news/politics/clearview-ai-rcmp-facial-recognition-1.5482266

Tunney, C. (2020, March 9). RCMP says it will limit its use of facial recognition tech - but won't stop using it entirely. *CBC News.* https://www.cbc.ca/news/politics/rcmp-clearview-ai-1.5490988

Tunney, C. (2021, June 15). RCMP's use of facial recognition tech violated privacy laws, investigation finds. *CBC*. https://www.cbc.ca/news/politics/rcmp-clearview-ai-1.6060228

Tyler, T. R., & Huo, Y. J. (2002). *Trust in the law: Encouraging public cooperation with the police and courts*. Russell Sage Foundation.

Tyler, T. R. (2006). Psychological perspectives on legitimacy and legitimation. *Annu. Rev. Psychol., 57*, 375-400.

UK Parliament. (2023, December 11). Committee launches an investigation into live facial recognition. *UK Parliament*. https://committees.parliament.uk/committee/519/justice-and-home-affairs-committee/news/198902/committee-launches-an-investigation-into-live-facial-recognition/

United States Department of Transportation. (2023). Promising Practices for Meaningful Public Involvement in Transportation Decision-Making. *USDOT*. https://www.transportation.gov/sites/dot.gov/files/2023-11/Promising%20Practices%20for%20Meaningful%20Public%20Involvement_2023Update_FINAL.pdf

Unsworth, K. (2014). Chain of command: Information sharing, law enforcement and community participation. *iConference 2014 Proceedings*.

Vagstad, S. (1995). Promoting fair competition in public procurement. *Journal of Public Economics*, *58*(2), 283-307.

van Duijn, S., Bannink, D., & Ybema, S. (2022). Working toward network governance: local actors' strategies for navigating tensions in localized health care governance. *Administration & Society*, *54*(4), 660-689.

Van Grembergen, W., De Haes, S., & Guldentops, E. (2004). Structures, processes and relational mechanisms for IT governance. In *Strategies for information technology governance* (pp. 1-36). Igi Global.

Van Steden, R., & Sarre, R. (2007). The growth of privatized policing: Some cross-national data and comparisons. *International Journal of Comparative and Applied Criminal Justice, 31*(1), 51-71. DOI: 10.1080/01924036.2007.9678760

Van Steden, R., & Sarre, R. (2020). The growth of privatized policing: Some cross-national data and comparisons. In *Regulating the Security Industry* (pp. 9-29). Routledge.

Vecchione, B., Levy, K., & Barocas, S. (2021). Algorithmic auditing and social justice: Lessons from the history of audit studies. In *Equity and Access in Algorithms, Mechanisms, and Optimization* (pp. 1-9).

Venturini, T. (2010). Diving in magma: how to explore controversies with actor-network theory. *Public Understanding of Science*, *19*(3), 258-273.

Vestby, A., & Vestby, J. (2021). Machine learning and the police: Asking the right questions. *Policing: A Journal of Policy and Practice*, *15*(1), 44-58.

Walby, K., & Larsen, M. (2012). Access to information and freedom of information requests: Neglected means of data production in the social sciences. *Qualitative Inquiry*, *18*(1), 31-42.

Walker, S. (1977). *A critical history of police reform* (pp. 141-45). Lexington, MA: Lexington Books.

Walker, S. (2016). Governing the American police: Wrestling with the problems of democracy. University of Chicago Legal Forum, 2016(15), 615– 660.

Walsh, D. P., J., & Conway, V. (2011). Police governance and accountability: overview of current issues. *Crime, Law and Social Change, 55*(2-3), 61-86. https://doi.org/10.1007/s10611-011-9269-6

Walton, H.D. (1982). Some recent advances in police technology. *Medicine, Science, and the Law*, *22*(1), 2-15.

Wang, H., & Ran, B. (2021). Network governance and collaborative governance: A thematic analysis on their similarities, differences, and entanglements. *Public Management Review*, DOI: 10.1080/14719037.2021.2011389

Wang, H., Qi, H., & Ran, B. (2022). Public–private collaboration led by private organizations in combating crises: Evidence from China's fighting against COVID-19. *Administration & Society 54*(1), 3–28. doi:10.1177/00953997211009890.
https://www.thestar.com/news/canada/opp-confirms-use-of-controversial-facial-recognition-tool-clearview-ai/article_8e8154ac-ddfc-51ca-9771-14919a946f3f.html

Wareham, J., Fox, P. B., & Cano Giner, J. L. (2014). Technology ecosystem governance. *Organization Science*, *25*(4), 1195-1215.

Weible, C., & Sabatier, P.A. (2007) A guide to the advocacy coalition framework. In: Fischer F, Miller GJ and Stanley MS (eds) *Handbook of Public Policy Analysis.* Boca Raton: CRC Press.

Weisburd, D., & Braga, A. A. (Eds.). (2019). *Police innovation: Contrasting perspectives*. Cambridge University Press.

Welle, D. (2021, September 7). German police secretly bought Pegasus spyware. *dw.com*. https://www.dw.com/en/german-police-secretly-bought-nso-pegasus-spyware/a-59113197

Westley, W. A. (1955). Secrecy and the Police. *Soc. F.*, *34*, 254.

Westmarland, L., & Conway, S. (2020). Police ethics and integrity: Keeping the 'blue code'of silence. *International Journal of Police Science & Management*, *22*(4), 378-392.

White House. (2023, May 22). *G7 Hiroshima Leaders' communiqué*. The White House. https://www.whitehouse.gov/briefing-room/statements-releases/2023/05/20/g7-hiroshima-leaders-communique/#:~:text=We%2C%20the%20Leaders%20of%20the,course%20for%20a%20better%20future.

Wilson, C. (2022). Public engagement and AI: A values analysis of national strategies. *Government Information Quarterly*, *39*(1), 101652.

Worden, R. E., & McLean, S. J. (2017). *Mirage of police reform: Procedural justice and police legitimacy* (p. 268). University of California Press.

Wortley, S., & Owusu-Bempah, A. (2022). Race, police stops, and perceptions of anti-Black police discrimination in Toronto, Canada over a quarter century. *Policing: An International Journal*, *45*(4), 570-585.

Wright, J. E., & Houston, B. (2021). Accountability at its finest: Law enforcement agencies and body-worn cameras. *Public Performance & Management Review*, *44*(4), 735-757.

Wynne, B. (2001). Creating public alienation: expert cultures of risk and ethics on GMOs. *Science as culture*, *10*(4), 445-481.

Wynne, B. (2006). Public engagement as a means of restoring public trust in science–hitting the notes, but missing the music?. *Public Health Genomics*, *9*(3), 211-220.

Yang, K. (2020). Unprecedented challenges, familiar paradoxes: COVID-19 and governance in a new normal state of risks. *Public Administration Review 80*(4), 657–664.

Zahariadis, N. (2003). *Ambiguity and choice in public policy: Political decision-making in modern democracies.* Washington, DC: Georgetown University Press.

Zheng, Q. (2023). Restoring trust through transparency: Examining the effects of transparency strategies on police crisis communication in Mainland China. *Public Relations Review*, *49*(2), 102296.